KnowBe4



CASE STUDY

Neoway and KnowBe4—Building a Culture of Security

Neoway is an influential B2B technology organization in Latin America. This Brazilian organization is the market leader for its big data analytics and AI platform, working with clients across more than 20 industry sectors including finance, automotive, consumer goods, oil & gas, technology and more. The organization has come to understand the critical nature of building a culture of security within its rank and file.

An Opportunity to Make Security Strategic

In 2018, Neoway had 400 employees, and its very small Information Security (InfoSec) team reported into the engineering department. Despite having hundreds of workers and being on a growth trajectory, Neoway operated as a startup in some ways.

The InfoSec team knew changes were needed. As a well-known B2B technology organization with a growing workforce that sometimes operated outside of their specific job role, the InfoSec team was concerned that Neoway could be a target for cyber attacks, notably phishing emails. The InfoSec team was strategically shifted from the engineering team to report directly to the CEO. Neoway also hired talented security professionals, including Flavio Costa, the organization's chief information security officer (CISO), who could help position Neoway's security programs as critical business drivers. One of his first jobs was to put a security awareness training program in place.

"KnowBe4...was extremely sophisticated, customizable and affordable—exactly the type of program we wanted to run."

"We have an entrepreneurial spirit here—if work needs to be done, people jump in to get it done regardless of their job description," Costa says. "That makes us very agile and efficient, but it does open the door to some risk."

Neoway

Industry

Big Data and Al Technology Platform

Headquarters

Florianópolis, Brazil

Challenge

Company growth makes it a target for cyber attacks and needed to pivot from startup mindset to a strategic culture of security.

Success by the Numbers

- Monthly training, including viewing new episodes of "The Inside Man"
- Hundreds of monthly phishing tests
- Organization wide Phishprone Percentage reduced from 20% to 3%
- Click-to-report ratio moved from 150:10 to 6:300, showing that employees improved their ability to spot phishing emails while simultaneously reporting them to the InfoSec team
- Overall reduced cost because no longer paying per campaign

The InfoSec team initially contracted with El Pescador, a security awareness training vendor they had previously worked with.

KnowBe4 Brings Power and Control

Timing was on Neoway's side. Almost immediately after bringing on El Pescador, the organization was acquired by KnowBe4, making Neoway the first KnowBe4 customer in Brazil.

As good as its experience with El Pescador had been, Costa was happy to transition to the KnowBe4 platform.

"We were very serious about security awareness within Neoway, and needed a security awareness training platform that helped us achieve our goals. KnowBe4 was that platform," Costa says. "It was extremely sophisticated, customizable and affordable—exactly the type of program we wanted to run."

The security awareness program that Costa and his colleagues created was focused on teaching employees how cybersecurity is important to the business.

"It was critical that our workforce understood how protecting the business from cyber threats was important to our overall business success and that all of us need to play a role in doing so," Costa says.

"Because we had so much control in how and who we tested with KnowBe4, we learned so much about our employees' habits."

Costa put a robust security awareness training and simulated phishing program in place that tested employees with phishing emails covering four different types of messages: those from Neoway systems such as G Suite, messages from the HR department or management, emails from recognizable partner organizations, and common phishing topics that are happening in the wild. They also tested different types of phishing campaigns against different employee departments. "Because we had so much control in how and who we tested with KnowBe4, we learned so much about our employees' habits and what tempted them to click," Costa says. "Simulated phishing emails from our HR department and from our internal systems like G Suite were the ones that people clicked the most. It was a huge help to have an idea of what made an employee want to click."

Almost equally important? Costa learned that employees were not reporting when they suspected a fraudulent email or link.

Costa continued, "We were able to see that only about 10% of employees were using the Phish Alert Button to report back to our InfoSec team. With this information we could incorporate into our trainings how important it is to report suspicious emails."

Making Calculated Decisions with PhishER

With a robust security awareness program in place that trains employees monthly and pushes simulated phishing tests multiple times per week, Costa was ready to move into an even more advanced direction.

"We taught our employees that reporting suspicious email...was something they could do to improve the health of our organization."

"We taught our employees that reporting a suspicious email—whether it was a real phishing email or a simulated KnowBe4 test—was something they could do to improve the health of our organization," Costa says. "Over time, though, there would be occasions where we'd have 300 employees report something to our InfoSec department, which was great, but also overwhelming."

That's when Neoway incorporated **PhishER**, a lightweight Security Orchestration, Automation and Response (SOAR) platform that manages the high volume of potentially malicious messages reported by users.

According to Costa, "PhishER helps our InfoSec team be more deliberate. It puts the reported emails into a queue and prioritizes them for us so we can work on the most important ones first. With it, we are able to be more efficient and better protect our organization by working on the highest threat messages first."

To further move the InfoSec department into position as a strategic business division, Costa also introduced KnowBe4's Virtual Risk Officer (VRO) to Neoway.

"KnowBe4 helped us train our employees, then test them. Then PhishER made it easy to report threats and put us in a position to better assess the health of our networks against phishing threats," Costa says. "Adding KnowBe4's VRO was a calculated move to help us get a better, more nuanced understanding of our risk posture."

VRO gave Neoway detailed information in dashboard format to illustrate the risk that individuals, departments, job functions and groups pose. Because employees are consistently being trained and tested, their Risk Scores rise and fall, giving Costa and the InfoSec team the opportunity to pinpoint if there is remediation needed in a specific area.

"Adding KnowBe4's VRO was a calculated move to help us get a better, more nuanced understanding of our risk posture so we can further protect our business."

Creating Awareness, Behavior and Culture

Costa put a thoughtful security awareness training program in place. But, because KnowBe4 is the de facto source on security culture, they complemented this program with another goal.

"KnowBe4 introduced us to their security culture experts, which was game changing for us."

"Initially, we wanted our employees to learn how to protect the organization from phishing threats, which KnowBe4 has helped us achieve, however, we've gotten so much more out of our relationship with KnowBe4," Costa says.

"KnowBe4 introduced us to their security culture experts, which was game changing for us. As far as I'm concerned, Perry Carpenter from KnowBe4 is the most important person in information security today because he is such an authority on transforming how people see security, identifying their behaviors about it and understanding how they react to it," Costa says. "Because of KnowBe4, we changed the name of what we do. We no longer run a security program. We run a security awareness, behavior and culture program."

Costa knows that an organization is never 100% secure. But, because of the KnowBe4 simulated phishing and security awareness training platform, PhishER and VRO they know they are doing what they can to protect Neoway's digital assets.

"Because KnowBe4 has helped us understand why security culture is so important, we've built a very unique and stable cultural foundation that only helps our organization," Costa says.