CASE STUDY

Cofense and AES

Multi-Language, Global Phishing Defense for Critical Infrastructure

COFENSE™

Cofense Case Study

COFENSE AND AES CORPORATION

Summary

AES turned to Cofense to support their awareness testing of 19,000 employees and contractors across 17 countries in multiple languages. Using a combination of Cofense PhishMe® and Cofense Reporter®, AES has seen strong improvements in the recognition of suspicious emails, decreasing its workforce's susceptibility while increasing the reporting of real phishing threats.

Executive Summary

Client: The AES Corporation, a multinational energy company

Challenges: Protecting a multilingual, multicultural and geographically dispersed workforce of employees and third-party contractors

Solutions: Cofense PhishMe, Cofense Reporter

Results: Substantial improvements in employee awareness, resiliency and reporting of suspicious emails.

Background

The AES Corporation is a Fortune 200 multinational energy company that generates and distributes electricity across 17 countries and four continents using a broad portfolio of fuels and technologies, including market-leading battery-based energy storage. With revenues of $14 billion and $36 billion in assets, AES has a workforce of 19,000 employees and contractors.

Challenges

With locations, employees and cyber-defenses scattered throughout the world, AES needed effective and easily customized anti-phishing training support. This meant running phishing simulations to condition employees who speak many different languages—English, Spanish, Portuguese, Vietnamese and Bulgarian, to name a few—and who work in diverse environments with varying cybersecurity regulations.

"Cofense recently reported that 91% of cyberattacks start with a phishing email," says David Badanes, Director of Cybersecurity Strategy at AES. "On the defensive side, we have to be right 100 percent of the time. Conditioning our people not to click malicious emails is critical to our primary value of safety."

> "Partnering with Cofense has considerably improved our cybersecurity stance at AES."
>
> **— Scott Goodhart, VP & Global CISO, AES**

Scott Goodhart, Vice President & Global CISO, points out that, as a global energy supplier, AES is part of the world's critical infrastructure: "One hit can impact the lives of the people whose electrical needs we service."

The Cofense PhishMe Difference

Before deploying Cofense PhishMe in 2016, AES worked with a different anti-phishing solutions provider. "The results were unremarkable," recalls Goodhart. "But then we were introduced to Cofense, and the level of sophistication in their approach was apparent. It's the difference between saying something and building a culture around something. Because of our partnership with Cofense, I now have employees who are much more skilled at identifying phishing emails."

> "It's the difference between saying something and building a culture around something. Because of our partnership with Cofense, I now have employees who are much more skilled at identifying phishing emails."
>
> **— Scott Goodhart, VP & Global CISO, AES**

Multi-language Support

Currently, 19,000 people in 17 countries are being trained to recognize and report phishing threats. With each simulation, AES personnel become more adept at spotting potential phishing indicators such as misspellings, unnecessary hyperlinks and attempts to play on people's emotions.

"What's especially impressive is that AES has gradually increased the complexity of simulated phishes, and the level of awareness among employees has continued to grow," notes Goodhart. "It's no easy feat, considering the simulations cover people in different age groups with varying degrees of technical savvy as well as different languages and cultures. This requires each simulation to employ a fair amount of customization."

Cofense Reporter and Cofense Professional Services

AES also uses Cofense Reporter, a solution that allows for quick user reports of phishing attempts. With Cofense Reporter, AES personnel simply click an icon to send suspicious emails to their company's security team for analysis. This generates streams of human-based phishing intelligence to aid in threat detection and speed incident response for security operations teams.

To develop custom reports and further enhance their phishing defense program, AES relies on Cofense Professional Services. For example, a Cofense consultant showed the AES team how to use different tactics in creating phishing simulations and to tailor phishes by region and language.

An "Exemplary" Approach to Cybersecurity

According to Badanes, if the company had to decide on only one cybersecurity training component to keep, it would be Cofense simulations. He believes these simulations exemplifies AES' primary value of safety and the company's approach to cybersecurity.

"Cyber events could cause physical damage and—potentially—loss of life," he says. "With electrical power, you must put safety first. Meaning both physical safety and cybersecurity. We train every person in our organization to think about ways to be cyber safe because cybersecurity is everybody's job." Attackers, he notes, will keep trying to come up with ways to get into networks. "Cofense helps ensure they don't succeed."

COFENSE

W: cofense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175