CASE STUDY

Cofense Case Study

# Protecting the Energy Grid from Phishing Attacks with Cofense

# Cofense Case Study

PROTECTING THE ENERGY GRID FROM PHISHING ATTACKS

## Background

A diversified energy and utility company with more than $30 billion in assets and operations in 25 states. The company operates regulated utilities and electricity generation through two primary lines of business and includes eight electric and natural gas utilities, serving 3.1 million customers in New York and New England. The organization operates 6.3 gigawatts of electricity capacity, primarily through wind power, across the United States, as well as employs 7,000 people.

### Executive Summary

**Client:** A U.S. based energy company with $30 billion in assets.

**Challenges:** Protecting the energy grid and preventing phishing attacks

**Solutions:** Cofense PhishMe, Cofense Reporter

**Results:** Reducing phishing susceptibility rates and significantly improving employee resilience and awareness

## Challenges

Energy providers face a cybersecurity double whammy: An attack could cut power to thousands of customers and cause millions of dollars in damage. And, since the company is subject to North American Electric Reliability Corporation Critical Infrastructure Protection (NERC/CIP) regulations, it risks incurring fines up to $1 million per violation per day.

> “If Cofense can help us defend against potential data breaches, and help us keep the lights on and the natural gas flowing for our customers, that’s a big deal”
>
> **— Cybersecurity Awareness Manager, $30B U.S. Energy Company**

Prompted by the increasing regulations and a recent scare, the company formed a dedicated security team to handle physical and cyber security, reporting directly to the CEO in 2012 with a key responsibilities around educating users about cyber safety. A comprehensive risk assessment conducted at the time showed “phishing is a real and present danger” for the company, so the organization needed an anti-phishing solution that could both educate users and help prevent phishing attempts. “Employee awareness and training became a major plank in our security platform,” according to the cyber security manager.

# Solutions

## Choosing Cofense PhishMe®

An anti-phishing solution had to meet several criteria – ease of use, a good value, compatibility with other systems, and actionable data delivery. After evaluating a handful of solutions, the company decided to conduct a limited proof of concept of Cofense PhishMe. The results sold the energy company on Cofense PhishMe.

A cloud-based SaaS immersive learning platform, Cofense PhishMe works easily with all major web browsers. It instructs users on the dangers of phishing through periodic simulations. Users have to decide if suspected phishes are legitimate or report them as suspicious. "Because we are a global company, we looked for a phishing platform that was extensible. Cofense PhishMe fit that bill because of its worldwide presence and multi-language capabilities," the cyber security manager says.

# Business Results

## Initial Reluctance

The organization's management originally pushed back on the idea of simulations. "People were concerned about our employees' perceptions of ethical phishing – that perhaps we were trying to entrap them and be punitive," the manager recalls.

"We had to win the hearts and minds of our executive team, so we showed them the amount of phishing and spear phishing emails that were getting into our system. And we emphasized the risk these phishing emails posed to the company, and we got them to agree to a pilot program."

The Corporate Security team also agreed its phishing simulations would cover everyone, from the CEO to the mailroom clerk, and there would be no punishment for employees dubbed "frequent fliers" – those who continually fail the tests.

But what really sealed the deal was a real spear phishing email sent to the CFO, allegedly from their CEO, requesting a money wire transfer. "Our CFO had been trained by being exposed to our simulation scenarios. The email didn't feel right to him so he reported it to our cybersecurity team. That was concrete proof of the value of our ethical phishing program."

## Simulation Program Success

The energy company launched its simulation program on a small scale by targeting company executives and their assistants. Over an eight month period, they expanded it to include HR, customer service, legal, corporate security and finance personnel. Each time, the phishing team shared results and susceptibility levels with management. It soon became clear departments that had already experienced phishing simulations had lower susceptibility rates. This proved that training and simulations work.

As simulations continued, department heads became invested in the program, even treating it as a competition. Our chief legal counsel, whose staff had scored particularly high, the manager says, "sat everybody down, put them through extra training and really emphasized the importance of understanding the effects of a potential phishing attack. Ever since that meeting, his group has consistently scored among the lowest susceptibility rates in the company."

Each Cofense PhishMe test generates lots of useful data. The cyber security manager leverages it to identify which departments might need some extra attention. “We use these data to help us plot out our itinerary for one-on-one meetings, so I can say, ‘Let’s start with the 10 facilities that have higher-than-average susceptibility to phishing, and go from there,” notes the manager.

“Using more of the available data has helped increase the return on our phishing investment. When I can show that nearly 400 employees downloaded a suspicious attachment in one hour, it really raises eyebrows,” the manager says. “Cofense PhishMe provides us with so much data that if you really dig into them and do a thoughtful analysis, they can be very useful.”

Since leveraging Cofense, the energy company has seen employee susceptibility trends decline.

### Future Efforts

Management reluctance is no longer a problem, and the manager recalls company executives are very strong supporters and are on board for implementing Cofense Reporter® across the enterprise. “Reporter will provide a very easy and well-defined process our employees can use to report suspicious emails.” Our current reporting process isn’t as well-known and therefore isn’t as well-used as it should be, he says.

“Deploying Cofense Reporter will give us the chance to reach out to all of our employees, reiterate the dangers of spear phishing, teach them how easy it is to report suspicious email, and encourage them to do it - often.” Cofense Reporter also should help improve their visibility into the phishing threat landscape considerably, allowing IR teams to respond quickly should a large-scale attack take place.

The energy company also has been developing its cyber security awareness training – using Cofense CBFree  - to reduce susceptibility of its “frequent fliers.” As the Company continues to develop its training curriculum, the Cofense Team has promptly provided whatever help needed. “I’ve been very impressed with the expertise, the cooperation and rapid assistance we get from the Cofense team,” notes the cyber security manager.

## Conclusion

The manager says in theory, the energy company could lose $3 billion in market valuation if it suffered a serious data breach. “If Cofense can help us prevent that, and if it can help us keep the lights on and the natural gas flowing for our customers, that’s a big deal.”

The company has calculated the cost of each simulation at approximately 60 cents per employee. That’s a reasonable price, considering the improvements in susceptibility rates and the attacks the company may have already averted thanks to heightened phishing awareness, the manager says.

“Because we work for an energy services company, we have a duty to protect the grid. One of the ways we do that is by encouraging our employees to step up and accept that higher responsibility – to teach them to stop and think before they download an attachment, for instance. And we believe Cofense will continue to help us do that and prevent bad things from happening.”

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise.

COFENSE

**W:** cofense.com/contact **T:** 703.652.0717
**A:** 1602 Village Market Blvd, SE #400
Leesburg, VA 20175