CASE STUDY

Cofense Case Study

Helping Multi-State Energy Utility Defend Against Cyber Threats Using Human-Generated Intelligence

COFENSE™

Cofense Case Study

COFENSE AND MULTI-STATE ENERGY UTILITY

Background

This large Midwestern-based company holds $4 billion in assets and provides energy services to more than 5 million customers in its multistate service area. The company, which employs 650 people, owns more than 9,000 miles of energy transmission lines with more than 500 substations.

Executive Summary

Client: U.S.-based multistate energy utility

Challenges: Preventing phishing attacks to protect $4 billion in power transmission assets.

Solutions: Cofense PhishMe, Cofense Reporter, Cofense Triage

Results: Significantly reducing the security team's time spent investigating suspected phishing emails.

Challenges

With the growing threat of phishing attacks looming, company leaders took stock. They realized that if a utility was hit by a cyberattack, it could potentially affect thousands of customers. They knew technology alone wouldn't solve the problem. They also knew they would need an effective program to condition user behavior to combat phishing risks.

> "When it comes to phishing, the email goes directly to your computer. What's the one way to stop people from clicking on them? Change their behavior."
>
> **— Cybersecurity Engineer, U.S.-based Energy Utility**

"We can put as many blocks in place in our network as we want. We can patch our servers and workstations, but there really is no patch for the human brain. When it comes to phishing, the email goes directly to your computer. What's the one way to stop people from clicking on them? Change their behavior," says the company's lead cybersecurity engineer. A solution with a strong behavioral conditioning component, he explains, not only trains users to recognize major security threats but also helps empower them to defend the company.

Deploying Cofense PhishMe®

After evaluating several options, the company decided to deploy Cofense PhishMe to launch an anti-phishing program. Cofense PhishMe is a cloud-based SaaS immersive learning platform that instructs users on the dangers of phishing through periodic simulations. Users who fail the test by clicking on links within simulated phishing emails receive instruction on how to identify, avoid, and report any threats they come across.

Deciding factors included the solution's prepackaged user education and ease of creating simulation scenarios. "The technology was fairly easy to deploy," says the company's information security consultant. "Once senior management approved our simulation program, we began by communicating with employees about what the phishing program was and what we expected from them. We reassured them we didn't intend to use their clicks or mistakes against them. We wanted the program to be a positive learning experience while increasing awareness of the threat." Simulations take place monthly. First the security team tests the chosen scenario on a select group of executives. If the executives approve the scenario, the simulation is sent to all employees.

Adding Cofense Reporter®

With the simulations under way, the number of suspected phishes reported to the help desk increased significantly. "Managing all the tickets manually was quite a challenge," the company information security consultant says. "So as soon as Cofense introduced the Cofense Reporter button, we started testing it. It was fairly easy to configure and roll out."

Cofense Reporter organizes and normalizes user reports of phishing attempts to improve threat detection. The solution, she says, makes it easy to report suspected phishes, saves the help desk an enormous amount of time, and provides invaluable user statistics. "An average of 60% to 70% of our employees use it to report our scenarios monthly."

> "Dealing with Cofense has been an all-around pleasant experience, thanks to the solutions' intuitive interface and the friendly, helpful Cofense staff."
>
> **— Information Security Consultant**

Implementing Cofense Triage™

After deploying Cofense Reporter, the company became interested in Cofense Triage, which extends Cofense Reporter's threat detection capabilities with a platform to respond to and analyze user reports of suspected phishes. Cofense Triage is available as a virtual appliance deployed on site or as a managed or cloud-based solution.

The need for Cofense Triage became evident as more and more users clicked the Cofense Reporter button to send suspected phishes to the help desk, the company's cybersecurity engineer says. "We needed some sort of tool to handle all this volume. I stumbled across Cofense Triage on Cofense's website. We set up a sales pitch call, and we were completely blown away. We got a proof of concept and have been in love with Cofense Triage ever since."

Business Results

The company uses the virtual appliance version of Cofense Triage, managed internally by the company's security team. According to the cybersecurity engineer, the biggest impact the solution has had on team operations is saving time. "It used to be that every single reported email would create a ticket. Then we'd have to take the time to look at the ticket."

With Cofense Triage, however, manual analysis is required only the first time someone reports a suspected phish. The security team analyzes it, and each consecutive time the same email is reported, Cofense Triage takes over. "I don't have to see it anymore. I don't have to go in and investigate it. It's just automatically categorized and dealt with," he says. He estimates Cofense Triage reduces analysis of suspected phishes from 17 clicks to five, a 70% increase in speed and efficiency for phishing analysis. "Twelve clicks doesn't sound like a whole lot, but if you've got a huge volume of emails, it's huge."

Cofense Triage works alongside leading malware analysis solutions that analyze suspicious files and URLs. "Cofense Triage performs really good analysis right upfront," he notes. "Using this capability saves time by quickly pulling information to determine if an email is a 'known bad' or 'known good.' That's always a great starting point to figure out how much time I really need to spend with each reported email."

The company makes use of three of Cofense's most popular solutions to create a full-scale defense against phishing risks. "Using Cofense PhishMe, Cofense Reporter, and Cofense Triage as an integrated suite gives us an efficient soup-to-nuts solution with scalable, out-of-the-box functionality to address the pervasive phishing threat," he says.

"Fantastic" UI

"Dealing with Cofense has been an all-around pleasant experience, thanks to the solutions' intuitive interface and the friendly, helpful Cofense staff," says the information security consultant. The cybersecurity team has been pleased with the interface of Cofense Triage, says the company cybersecurity engineer. "The Cofense Triage user interface is fantastic. It's really easy to use. Cofense developers have done a fantastic job of making it easy to write rules using the malware identification tool YARA. Everything you can see and need to write a rule is – either you're looking at it, or it's one click away."

The information security consultant says she's pleased with solutions' usability. "I am not a proficient programmer, and I can make Cofense PhishMe do everything we need it to do. The interface is straightforward. If I ever have a question, the Cofense customer success team has always been prompt in providing an answer." Cofense engineers have been just as helpful, according to the company's cybersecurity engineer. Cofense engineers were knowledgeable and efficient, he says, and they were instrumental in troubleshooting some minor integration challenges while deploying Cofense Triage.

Conclusion

The company's C-suite is happy with the Cofense implementations, says the company's cybersecurity engineer. The executive leadership team sees the value the monthly simulations bring to the company and the "surprise training" they deliver. Both managers and staff are happy when they correctly identify a phish. Many treat the program as a personal challenge. "When people get fooled by a monthly phishing simulation, someone might say, 'Oh, that was a good one,' and they'll want to make sure they do better next time."

Overall, he says, the Cofense solutions have helped fortify the company's defenses. As a utility, the company recognizes how critical it is to prevent any cyberattack. "Since phishing is the most successful method to initiate an attack, Cofense's end-to-end solution is extremely valuable to our security program's success."

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