SUCCESS STORY

Communications & Power Industries

Communications & Power Industries Delivers Job-Specific Cyber Awareness Training to Employees through Envigilant Systems Professional Services

Employees internalize security best practices through live hands-on exercises

Communications & Power Industries LLC

Communications & Power Industries (CPI) is a global manufacturer of electronic components and subsystems focused primarily on communications and defense markets. Founded in 1948 as the former Electron Device Business of Varian Associates, Inc., today CPI has several semi-autonomous divisions and employs approximately 2,000 people across the globe, with manufacturing facilities in the U.S. and Canada. Each division provides its own staff and administrative services overseen by the Palo Alto management team.

With about half its business geared toward government and military customers, CPI must ensure that it meets the requirements of the Defense Federal Acquisition Regulation Supplement (DFARS) security standards. "Security is an important piece of being a government contractor," says Amanda Mogin, Senior Director of Corporate Communications and Administration for CPI. "We have training requirements for both employee cyber awareness and IT incident response. We needed a program that is flexible enough and job-specific enough to make it worthwhile for our employees to do this training."

CPI found the customizable kind of training program it needs through Envigilant Systems, the professional services arm of Allied Telesis. "While attending a cybersecurity seminar, I saw a demonstration of a DECIDE training exercise and it seemed like something that is adaptable and scalable and it could be customized to meet our unique needs," says Mogin. "It would address the issues we were having in doing our cyber training through static PowerPoint presentations."

> We've had ongoing conversations on a number of different levels with Envigilant Systems team that have been very helpful. We have definitely used them as a source of best practices.

Amanda Mogin
Senior Director of Corporate Communications and Administration at CPI

Training scenarios are highly customized to employees' tasks

The Envigilant Systems team delivers a robust, highly customizable cyber awareness program consisting of live exercises that enable workers to learn, or reinforce what they know, about task-specific risks. The exercises, which are developed jointly by Envigilant Systems consultants and the customer organization, are crafted to challenge people in scenarios that mirror their own daily tasks. For example, an employee in Finance might be presented with an order to transfer funds and they need to decide if the order is legitimate or if it originated from a bad actor. An engineer might receive an email request from a colleague to share product design specifications and they must decide if this is a spoofed request attempting to steal intellectual property. The tests are customized to specific job roles to simulate the real work environment.

Employees who are tested with these dynamic real-world scenarios learn to apply security best practices to their critical job functions. They learn about attackers' tactics, techniques and procedures (TTPs) that are indicative of a potential cyber-attack. They also learn the appropriate ways their company wants them to respond to cyber incidents.

Allied Telesis/Envigilant Systems and the Norwich University Applied Research Institute (NUARI) collaborate to develop DECIDE platform exercises around NIST security standards. Exercises are delivered in classroom settings via a cloud service, so there is nothing for customers to buy or install. A service engagement includes consultation with Envigilant Systems professional services to construct the awareness exercises. Following the training, Envigilant Systems provides a summary report outlining the students' responses – without identifying individual students – and an analysis of the responses. This helps an organization understand its overall threat response readiness and fine-tune its policies and response playbook.

A more thoughtful approach to awareness training

Prior to working with Envigilant Systems, CPI used various methods to create cyber awareness among employees. “We had other training programs from other vendors—phishing simulations and video-based vignettes,” says Mogin. “For the annual desktop exercises, we developed the scenarios in-house and delivered the content largely by PowerPoint. Some students were in a classroom setting, while others joined over the phone. It wasn’t very effective because it was static, ‘one size fits all’ training. We had to make assumptions on how people would react to a scenario, and we ran the risk of losing control of the conversations and the lessons we wanted to impart.”

These old tools were largely preaching to the employees rather than engaging them. What’s more, Mogin says the people who joined by phone got less out of the experience because they weren’t actually able to actively participate. She says they were alienated by the listen-only approach.

With the training delivered via the DECIDE platform, everyone in the room has their own computer, and the scenarios are customized to their position and relevant to their job role. “The person in IT isn’t presented with a situation that’s only appropriate for a finance person, and a finance person isn’t seeing something that a marketing person would typically deal with,” says Mogin. “It allows people to think, ‘this is something that directly applies to my job. How would I respond?’ We can present much more thoughtful exercises for every individual in the room, and the people talk to each other just like they would in real life. It’s a very collaborative and comprehensive approach to training.”

What CPI learned from running the scenarios

“We learned that our people generally know what to do and who to talk to in these scenarios, even if they couldn’t quote the exact language in the relevant policies,” Mogin says. “During the training, they were very appreciative for the opportunity to see things in a way that had no consequences. So, if they got an email and it was a bad email and they clicked on it, they learned that they shouldn’t have clicked and why, but thankfully there was no actual harm resulting from their actions.”

“We also learned that we have to do a better job of ensuring that people know the language in our policies, and that we need to do a better job of publicizing internally if a cyber incident does happen – even if employees aren’t directly involved – so that those incidents can end up being learning experiences for everyone.”

"We've had ongoing conversations on a number of different levels with Envigilant Systems team that have been very helpful," says Mogin. "We have definitely used them as a source of best practices. We ask questions like, 'What do you normally see here?' It's helpful to know if our results are inside or outside the scope of what is normally seen in these scenarios."

The engagement experience with Envigilant Systems

Mogin says she reached out to Envigilant Systems after seeing the DECIDE demonstration at a seminar. "We've been very surprised at the level of service they provide us. It seems higher than what we expected based on other vendor relationships," she says. "They brought three or four people to every meeting with us and talked through how they could help us. It wasn't just 'we can sell you this platform, here's what it costs.' They really wanted to understand what we do and what our training needs are and what would work for us."

> *It allows people to think, 'this is something that directly applies to my job. How would I respond?' We can present much more thoughtful exercises for every individual in the room, and the people talk to each other just like they would in real life. It's a very collaborative and comprehensive approach to training.*
>
> **Amanda Mogin**
> **Senior Director of Corporate Communications and Administration at CPI**

CPI has a very lean corporate staff. Using Envigilant Systems services allowed Mogin to show her management the value proposition of the cyber awareness program. "We know that cybersecurity readiness is everyone's responsibility, and all our employees must be involved in preventing, managing and responding to cyber events. By doing this training on a regular basis, we can prove to our government, military, and commercial customers alike that we are serious about cybersecurity. It's one more value statement we can pledge to all our customers."

Envigilant Systems
Secure IoT Solutions & Services

3041 Orchard Parkway, San
Jose, CA 95134, USA

1-800-424-4282

info@envigilantsystems.com

About Us

Envigilant Systems is a business unit within Allied Telesis that has engineering capabilities to build security-focused IoT solutions for manufacturing, transportation, and smart building applications. Backed by 30+ years' experience building secure, reliable networks, Envigilant Systems is ideally placed to design, implement and provide services for tailored solutions to meet demanding requirements. With a global sales and support network, Envigilant Systems is solving challenging IT problems worldwide.