There aren’t many production facilities in the country more secure than refineries. Leaders in the fuel and petrochemical industries pride themselves on workplace safety and security, which is evident based on even a cursory glance at any AFPM member’s annual security report.

An increasingly major part of maintaining safety and security at refineries, however, is investing in cybersecurity – a critical line of defense against worst-case, but thankfully rare, scenarios.

Earlier this month, 400-some college students across the country were faced with a simulated version of threats straight out of a James Bond supervillain’s playbook. At the Department of Energy’s 2018 CyberForce Competition, teams of students were charged with defending a simulated oil transportation network, a power delivery system and high-performance computing systems against real-time attacks generated by a team of cyber experts from the National Guard and several DOE national labs. AFPM served as a sponsor of the event.

The competing teams were assembled at national labs in Illinois, New York, Idaho, California, Tennessee, Washington and New Mexico, coordinated through video conference. A total of 70 institutions, including public, private and community colleges, participated, with each team composed of six players and a faculty coach.

The hacking part of the competition lasted eight hours, and each team also was required to provide documentation on their strategy and explain to a team of industry representatives why their method of security was best and how it would mitigate the hacks.

In this “Shark Tank”-style setup, I was fortunate enough to serve as one of those judges. In addition to being impressed by the diversity of the groups, I was overwhelmed by some of the outside-the-box thinking demonstrated by the students. It’s precisely the kind of thinking that AFPM member companies covet in cybersecurity specialists.

This generation of college students is eager to hit the ground running in a cutting-edge field. They’re motivated by the service of protecting others from attacks. They don’t want to sit in a cube and write code all day. And naturally, they’re interested in the financial rewards and stability that comes with cybersecurity. In the refining and petrochemicals industries, there is no shortage of employment opportunities that fit every one of those criteria.

Cybersecurity work in our industries gives students the chance to be part of a team, combating threats like the ones simulated at CyberForce. This work isn’t for the faint of heart — a software company might be a better fit for cybersecurity specialists uninterested in the kind of excitement refinery and petrochemical work provides. We want analytical workers who aren’t afraid to meet these challenges head-on.

AFPM member companies are extremely proactive on cybersecurity, with risk mitigation prioritized at

every facility. We also know that supporting STEM education is critical to preparing the next generation for important (and well-paying!) jobs in our industries well into the future. An event like CyberForce is the perfect training ground for emerging cybersecurity specialists interested in a career in fuel and petrochemical manufacturing. Needless to say, AFPM will once again be a proud sponsor of CyberForce when it reconvenes in November 2019.

Dan Strachan is AFPM's Director of Industrial Relations & Programs. He is a proud alumnus of the University of Central Florida, which just so happened to claim the top prize in the 2018 CyberForce competition. Go Knights!

Print as PDF:

Topics

Security

Cybersecurity

Facility Security

Workforce, Economy, & Manufacturing

Education & Training

Tags

CyberForce

STEM