“Information security is the immune system in the body of business.” This cybersecurity saying has gained new weight in 2020, with the COVID-19 pandemic reinforcing the need for cybersecurity to be robust, flexible and agile—just like a healthy immune system. And these requirements are especially crucial for fuel and petrochemical companies, since they are among the industries deemed critical for economic and national security by the Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

The onset of the COVID pandemic rapidly initiated a cascade of cyber challenges to go along with the dramatic changes affecting many other aspects of corporate life. This included an unprecedented number of fuel and petrochemical industry employees working remotely, a massive increase in COVID-related phishing and ransomware, and the increased use of onsite technology by facilities seeking to minimize in-person contact. All of these shifts expanded attack surfaces and potential cyber vulnerabilities.

The fuel and petrochemical industries, however, were nimble, had tools available to help address these challenges, and tailored responses to the unique challenges of their facilities.

As a result of their critical industry status, companies were already in contact with state and federal government cyber intelligence networks, with existing relationships and communications channels available to aid coordination as they faced these new challenges. Our industries work closely with CISA and others to identify, respond to, and mitigate cyber threats – and this partnership was bolstered during the pandemic.

Many companies also have extensive business continuity plans that contain relevant contingency preparations. Meaning that many companies had, for instance, already conducted load tests to ensure their virtual private networks (VPNs) could scale up to handle the increased number of remote logins as employees worked from home.

In addition to individual company and government-led preparations, the industries’ deep-seated culture of safety and preparedness has resulted in a longstanding practice of industry-wide information sharing. The Oil and Natural Gas Information Sharing and Analysis Center (ONG ISAC), a private sector cybersecurity hub that allows members to share information and coordinate against threats, is another valuable resource that AFPM and its members relied upon during the onset of the pandemic.

Still, the best-laid preparations require quick pivots to meet new demands. One such illustration of this during COVID included modifications to employee education practices, which were facilitated by existing communications channels and backed by company leadership. For example, cyber teams were able to use standing company-wide emails and meetings to highlight current threats and educate employees about warning signs. Companies also provided additional training and testing, including phishing simulations, to help employees adapt to new working conditions.

“Balance has always been the question in cybersecurity, specifically in terms of how much restriction is necessary to adequately protect the organization,” says Stephanie Franklin-Thomas, Chief Information Security Officer at Motiva Enterprises. “The COVID-19 pandemic has tilted that scale with the ‘new normal’ consisting of an increase in remote work. Thus, organizations must think about the amount of restriction in relationship to the biggest risk elements of cybersecurity: people. Developing organizational talent into active pseudo-members of our cyber defense, my Cybersecurity team can assist in balancing the restriction versus protection scale.”

The likelihood of ongoing remote work means that the cybersecurity and educational efforts triggered by the COVID pandemic are unlikely to lessen anytime soon, making a robust cybersecurity workforce more necessary than ever for the fuel and petrochemical industries. And while many are facing tight budgets in the wake of the economic shutdown, the need to continue investing in their company’s future via a healthy cyber immune system remains essential.

Equally critical, companies must continue to have the flexibility and autonomy to innovate and respond to ensure their facilities and employees stay safe. Overly prescriptive regulations hamper cyber experts’ abilities to meet the demands of the constantly evolving threat landscape. Restrictive policies could have adverse impacts not only for the employees and companies, but for the industries and economies that depend upon their crucial products.

Print as PDF:

Topics

Security

Cybersecurity

Tags

Cybersecurity

Network Security