ULTRA | Intelligence & Communications

Defend Critical Infrastructure from the Latest Cyber Attacks

Overview

We rely upon our critical infrastructure to supply us with everything from clean drinking water to reliable electricity to safe transportation. It's common to believe that our infrastructure is secure because until recently it has been. However, there is a new wave of threats aimed directly at our most vital infrastructures that are being carried out by nation states and terrorist groups.

These new threat actors are more sophisticated than ever and fully capable of using highly advanced techniques to compromise a variety of critical systems. After they gain access, they can go on to sabotage infrastructure in ways that are potentially life-threatening on a large scale.

In this whitepaper, we'll explore the current landscape of Critical Infrastructure Protection (CIP), do a deep dive into one particular close call in Florida, and discuss how Ultra technology can protect against these rapidly evolving threats.

Defend Critical Infrastructure from the Latest Cyber Attacks

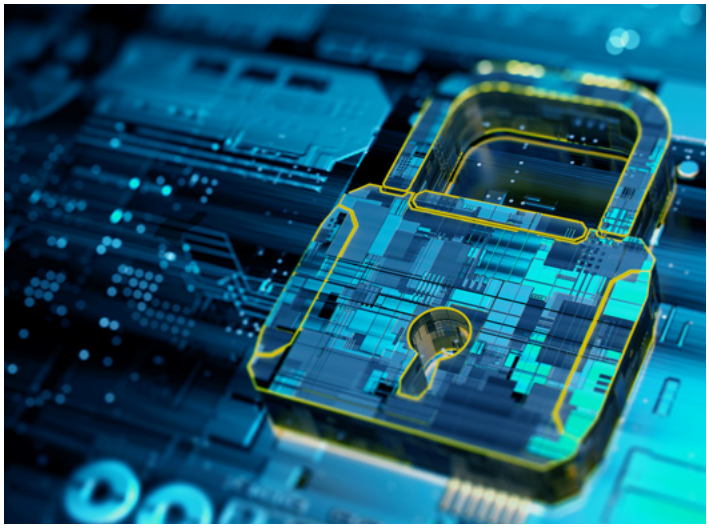
CIP Today

Experts define CIP as the need to protect the infrastructures we rely upon to provide us with food, electricity/power (including nuclear power), transportation (from roads and bridges to ports and airports) and water treatment facilities from natural disaster, terrorist activity and cyber-attacks. There are 16 identified sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water and Wastewater Systems

Each sector was assigned a supervising entity (Nuclear Reactors, for instance, fell under the Department of Energy) and directed to create and implement detailed plans for CIP. In 2006, those agency plans were combined into the National Infrastructure Protection Plan (NIPP). In addition, NIPP defined how public and private sectors can work together to achieve CIP best practices.

According to this IBM Report, attacks against operational and information technology increased 2000% in 2020 from 2019. That's a sobering statistic, and it doesn't bode well for the future. CIP sectors currently employ a range of best practices developed over the past two decades – but are those systems and practices enough to face these new and evolving threats?



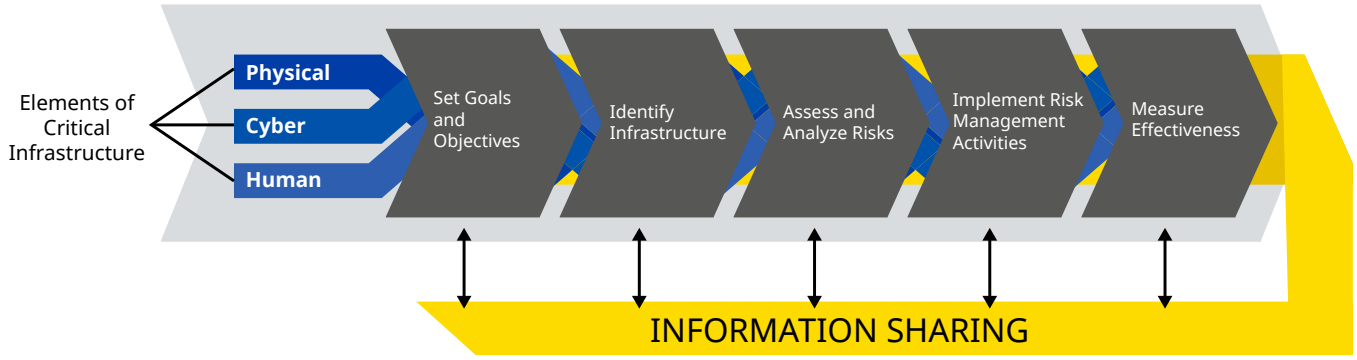
The Cybersecurity and Infrastructure Security Agency (CISA) outlines a list of best practices that are fundamental to CIP planning. They include:

- Establish goals and objectives
- Identify existing examples of relevant critical infrastructure security and resilience plans or programs
- Determine the scope
- Identify the stakeholders
- Document roles and responsibilities
- Establish coordination and information sharing mechanisms
- Set timelines
- Build a risk management framework
- Design and conduct assessments
- Conduct training and education, including exercises
- Establish metrics
- Promote the program through outreach and awareness

CISA updated these steps in 2019, when the prime driver behind CIP was incident response. While incident response is a aspect of CIP, it is still a reactive approach in these new days of sophisticated cyber threats.

In addition to sharing basic best practices, CISA also included a risk management framework to help clarify how to identify and mitigate risk.

Defend Critical Infrastructure from the Latest Cyber Attacks



By way of example, we'll examine a well-publicized attack in detail to see how terrorists seized power over a small Florida city.

Deep Dive into the Water System Hack

Oldsmar, Florida is a 15,000-person city, and in February of 2021 a group of unknown cyber assailants gained access to the water treatment plant – a critical infrastructure sector. The criminals used a remote viewing and control software typically used to troubleshoot IT problems or remotely monitor systems to alter the amount of caustic sodium hydroxide (or lye) that is released into the water supply.

As Wired magazine retells, the operator on duty noticed that his cursor was moving independently as assumed at first that it was his boss accessing his system to check it remotely. However, a few hours later he watched his cursor adjusting the levels of sodium hydroxide to a dangerous level. He quickly managed to change it back, but if the hacker had succeeded, they would have raised the concentration from 100 parts per million to 11,100 parts per million. At certain concentrations, sodium hydroxide causes severe tissue damage or even death.

Many in the cybersecurity community were appalled but unsurprised. This hack represented the first close call in the United States, with bad actors actively attempting to sabotage critical infrastructure to the point of potential loss of life. Most worryingly, at first they could not find the "hole" that the hackers used to gain entrance. The sheriff of Pinellas County (where Oldsmar is located) admitted that the operational technology (OT) was most likely accessed from the internet since OT systems were accessible externally.

Long-standing best practice is to segregate OT and IT in a CIP environment. Both, however, need to be secured from outside access. While the attack is the most public, there is evidence that hackers can easily discover these systems on the internet through tools like Shodan. While the sheer complexity of OT and IT systems deters many intruders, the savviest and most advanced can navigate them with ease.

It's not just water utilities that face attack. In 2015, the Russian hacker group Sandworm enacted cyber warfare against the Ukrainian power grid, opening circuit breakers and leaving more than 250,000 citizens in the dark. These famous examples only underscore the need to rethink how we approach CIP.

Securing OT and Safeguarding our Infrastructure

The most secure way to batten down OT is through the deployment of an industrial firewall. Ultra's CyberFence CIP solutions are award-winning industrial firewalls designed to protect OT networks in new and legacy systems against cyber-events that impact safety and system availability.

Our experience-based evaluations of end-to-end systems – from access control, surveillance to Layer 2/3 network security, malware protection, to PLC security – inform our vulnerability assessments to establish security levels that assure secure operational efficiency and effectiveness.

Defend Critical Infrastructure from the Latest Cyber Attacks

We design, build and deploy solutions that combine technology, policies and procedures to align risk with turnkey solutions that maximize systems spending while eliminating downtime due to breaches. When evaluating any cybersecurity solution, owners and operators of energy control systems are obliged to include North America Electric Reliability Corporation (NERC) compliance in the decision-making process. While many types of facilities are required to meet NERC standards, all principals in the industry should strive to comply for best security outcomes that assure potentially life-saving system stability.

Embedded systems and associated devices that run critical operations are vital to managing automation and control systems. These networks are complemented throughout industrial facilities by the OT domain which is the front-facing edge that blends cyber components with physical devices to form complex networks whose operational integrity is paramount to human safety. As a result, there is increasing pressure within Industrial Control Systems (ICS) organizations to allow IT departments to perform more cyber-related services in the ICS domain.

CyberFence CIP has several adaptable configurations:

- Industrial DPI Firewall with Layer 3 Encryption: EtherGuard
- Industrial DPI Firewall with Layer 2 Encryption: DarkNode
- High-speed Layer 2 Encryption: UltraCrypt
- Industrial DPI Firewall: EtherWatch

In addition, Ultra's solutions are approved by automation vendors and standards groups to assure the highest levels of protection. They work as part of the cyber kill chain, fencing in attackers and forcing them to work within the secured infrastructure, severely limiting their chances of sabotage.

CyberFence CIP integrates into existing systems to enable global deployment, while offering real-time information flow for innovative business models. It migrates into legacy infrastructure to speed value-oriented deployments. And, to avoid another remote access hack like the one in Florida, our solutions support safe remote access.

For more information on CyberFence CIP and our other crypto offerings, visit our home page.

With the rise of peer adversaries on the world cybersecurity stage, it is more important that ever to safeguard our critical infrastructure from attack. In the future, such attacks could be malicious on a much larger scale than poisoning the water of a small city. Future-proof OT now to defend against the attacks of tomorrow.

© 2021 Ultra Electronics Ltd. All rights reserved.
1048.1-I&C-en-REV1121

ULTRA | Intelligence & Communications

ultra.group