C A S E S T U D Y

Addressing the Next Threat to the Power Grid

Critical Infrastructure Cyber Security & NERC CIP Compliance

Problem:
The Next Threat is Already Here

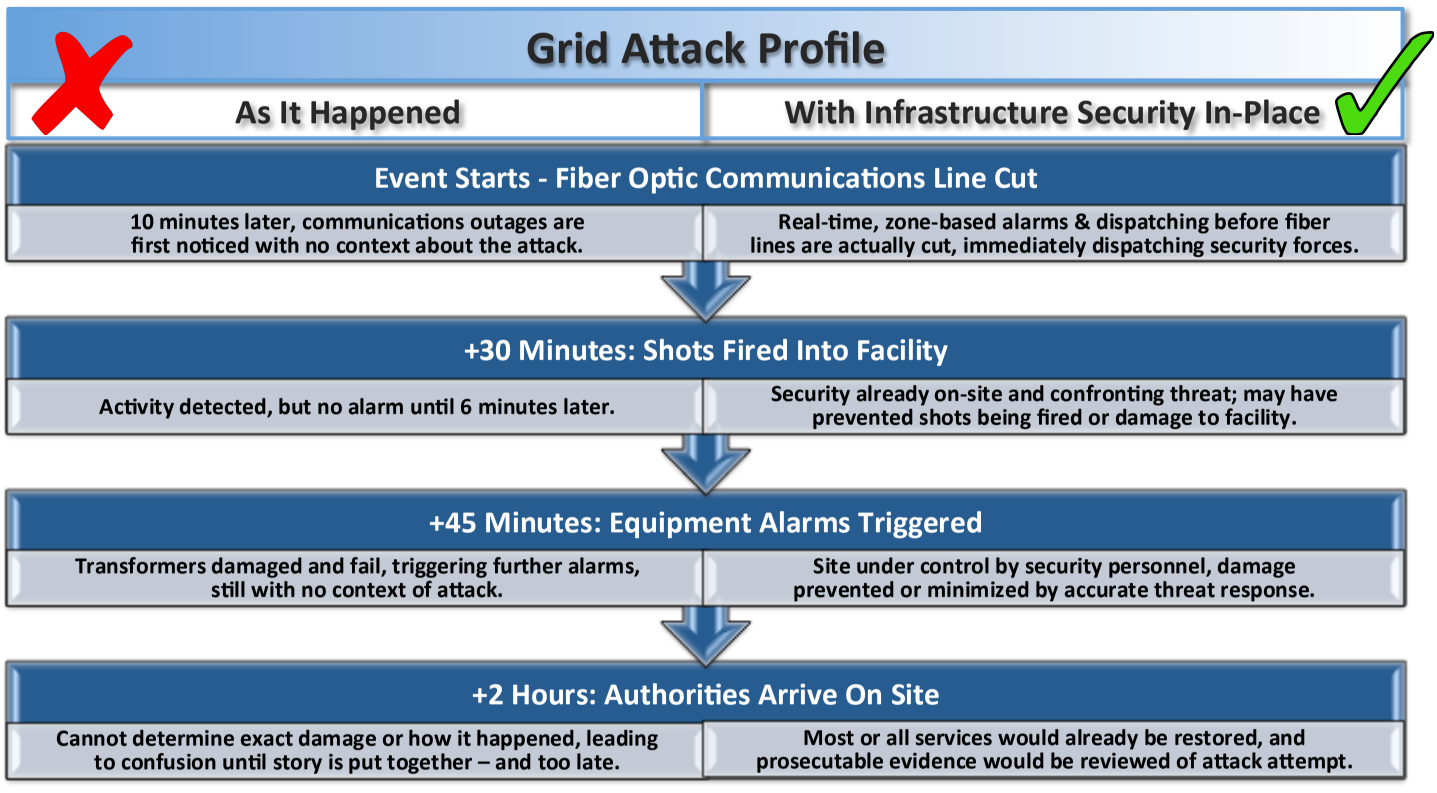
A new form of threat against the power grid has emerged. Recently, a terror-like attack against a California-based substation shut-down the operation of numerous transformers resulting in millions of dollars in damages, and an awakening of the entire industry to this previously under-publicized vulnerability. The remediation costs were not the extent of the financial impact; in the aftermath the regional power authority allocated $100M to harden its critical facilities against similar attacks as an FBI investigation left open the probability that this type of attack could potentially be carried out again.

The event initiated when the perpetrators cut the fiber-optic cables in underground vaults (manholes) outside of the substation, apparently to sever communications between the station and the outside. At that point, they waited to determine whether a response by law enforcement or security personnel was imminent. After a period of time in which no response was observed, firearms were used to damage transformers. Ultimately alarms were generated when the transformers failed, but the damage had been done.

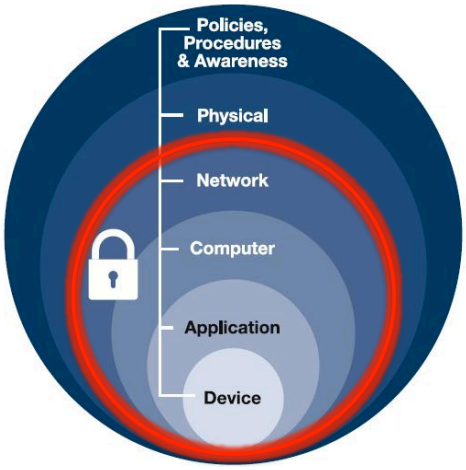
Solution:
Critical Infrastructure Cyber Security

What if the substation as well as law enforcement authorities had been notified the instant the attackers opened the manhole or handled the fiber optic cable prior to cutting it? What if these notifications automatically triggered additional security systems such as cameras to provide real-time situational awareness? What if the notifications could have simultaneously re-routed network traffic to maintain communications with the station? What if all of this were possible?

All of this is possible with proven solutions initially developed for the US Government and Military who long understood the threat of physical attacks to network infrastructure. These systems defend and protect critical networks from physical attacks enabling the real-time detection of intruders. Had these countermeasures been in-place at the California substation, a very different outcome would have resulted; authorities would have arrived in-time to thwart the attack. ***Critical Infrastructure Cyber Security*** is an additional layer of security which can provide front-line defense of critical infrastructures.



How the Power Industry Can Respond



Critical Infrastructure Cyber Security enables 24/7/365 real-time monitoring of network infrastructure and various points of vulnerability such as manholes, equipment cabinets, etc. Network Integrity Systems (NIS) is the industry leader within the government and military sector and has recently introduced a civilian version of the technology with the same features and functionality. Called ***Vanguard CS***, it is the first solution that monitors your infrastructure from the inside-out, and enables scalability and flexibility via software-defined infrastructure security and monitoring. The solution is the most cost effective way to address a multitude of threats to the heart of critical infrastructure and has been deployed by DoD, DHS, and many other government agencies for the past decade.

Cyber security compliance has become a critical priority for NERC CIP v5, and will become and even more integrated component of future standards. ***Vanguard CS*** provides these key capabilities in support of CIP compliance:

- ☑ **Visibility** across all platforms of the entire network, with real-time alerts of any physical interactions
- ☑ **Central Management:** a single pane of glass across the entire network, enforced via a Unified Security Policy that is zone-based (eg, according grouping of Cyber Assets, BES Cyber Systems, Impact Ratings)
- ☑ **Automation and network security** change management that is application and event-driven
- ☑ **Continuous compliance** with audit-ready reporting and evidence

Together, power authorities, NERC, and industry can leverage ***Critical Infrastructure Cyber Security*** to develop rigorous standards to integrate physical and network cyber security with real-time monitoring and threat response.

Early Power Authority Adoption Proving Successful

NIS recently worked with a regional power authority to address their SCADA network infrastructure security concerns. The engagement began with a pilot at one of their power stations located on an island subject to frequent flooding. During the winter months, the location was experiencing ice damage to the fiber optic cables used in their SCADA network to control power plant relays. NIS technology enabled the power authority to receive early warnings of deleterious affects on the infrastructure caused by nature. The pilot integrated ***Vanguard*** with the power authority's existing physical security system to provide real-time alerts regarding any cables being effected. This security measures prevents critical down-time for grid subscribers and any potentially devastating costs to the power authority caused by damage to critical SCADA cabling.

NIS additionally demonstrated how this capability prevents physical cyber attacks, can be scaled to provide security across multiple geographically dispersed sites, and trained the power authority on threat response. Now, the power authority is considering an expansion of the technology to take advantage of the full capabilities of ***Vanguard CS***, enabling the monitoring of multiple infrastructure pathways and communication cabling types across many zones. The digitization of the power authority's physical security monitoring into a centralized software monitoring dashboard will ensure continuous compliance and enable cost-effective scalability across their many critical sites.

Network Integrity SYSTEMS

WE BRING SECURITY TO LIGHT™

ABOUT NETWORK INTEGRITY SYSTEMS

Network Integrity Systems (NIS) develops and manufactures cyber security products that enable organizations to protect the integrity and availability of their critical network infrastructure as well as the data it carries. NIS' innovative, best-of-breed solutions include the INTERCEPTOR product line (for US Government) and the VANGUARD product line (for Private Enterprise and Non-US Government). For more information, visit ***www.networkintegritysystems.com****.*