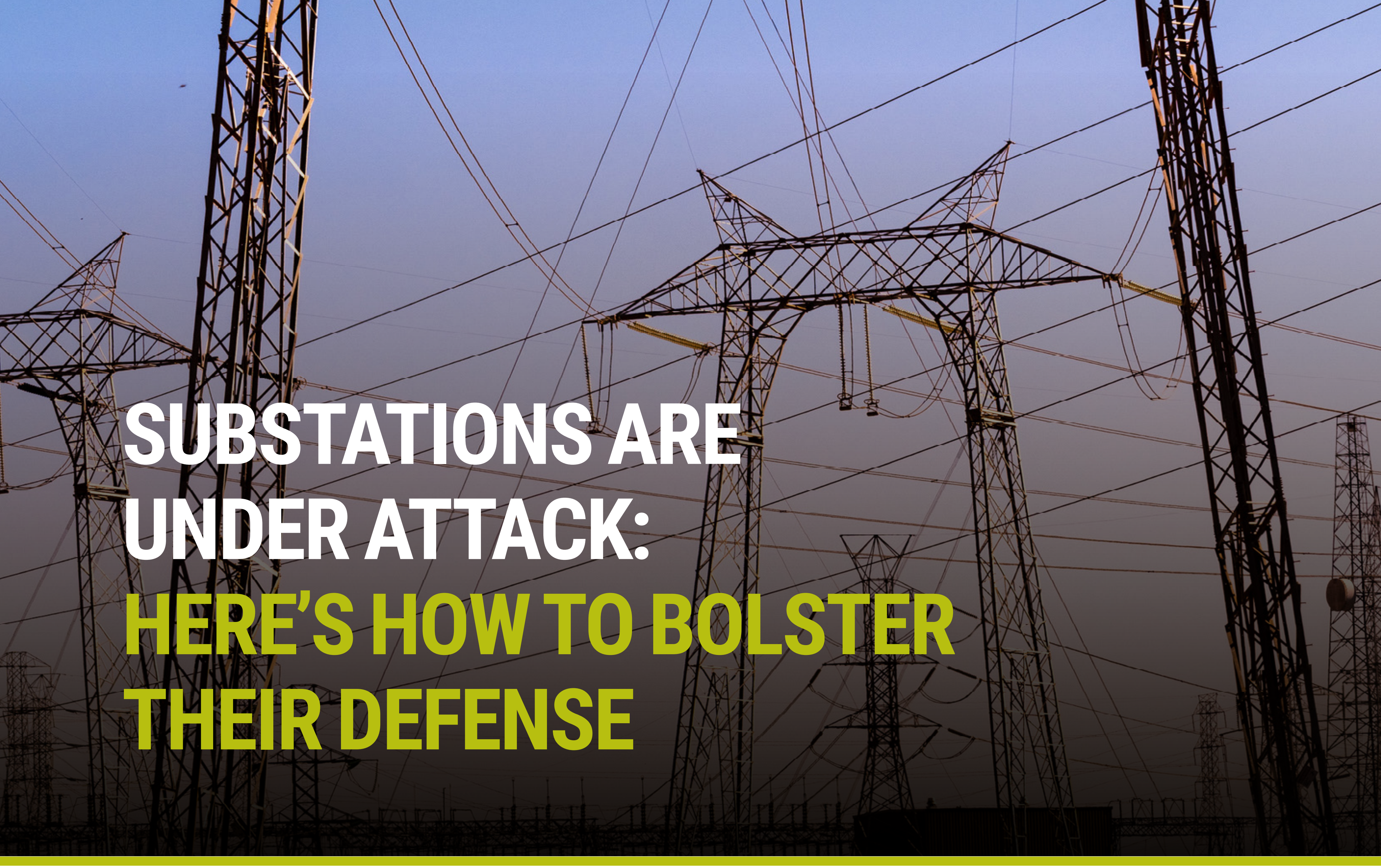


SUBSTATIONS ARE UNDER ATTACK: HERE'S HOW TO BOLSTER THEIR DEFENSE

MOTOROLA SOLUTIONS | UTILITY DIVE

Custom content for Motorola Solutions by studioID

In December of 2022, around 40,000 utility customers in Moore County, North Carolina suddenly found themselves without power.

Many people were left in the dark and cold for days, and the impact was sufficiently widespread that the county declared a state of emergency and opened up a shelter to serve meals and provide showers and laundry facilities to those who had been dislocated.

The combination of an aging grid and increasingly severe weather has already caused an increase in power outages. But the loss of power in North Carolina wasn't caused by a storm: instead, the outage was caused by an armed attack on two substations. Unfortunately, the malicious targeting of substations in Moore County was not an isolated incident. Over the past year, attacks on substations in Washington State and Oregon led to power outages impacting tens of thousands of people. The Federal Bureau of Investigation (FBI) recently thwarted a planned attack on substations in Maryland that was designed to destroy the city of Baltimore.

While many attacks on substations are never reported publicly, it's clear that concerns about the vulnerability of this essential grid infrastructure is on the rise. Both the Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) have singled out attacks on the grid, including substations, as a popular tactic among people seeking to foment societal unrest and inflict economic damage.

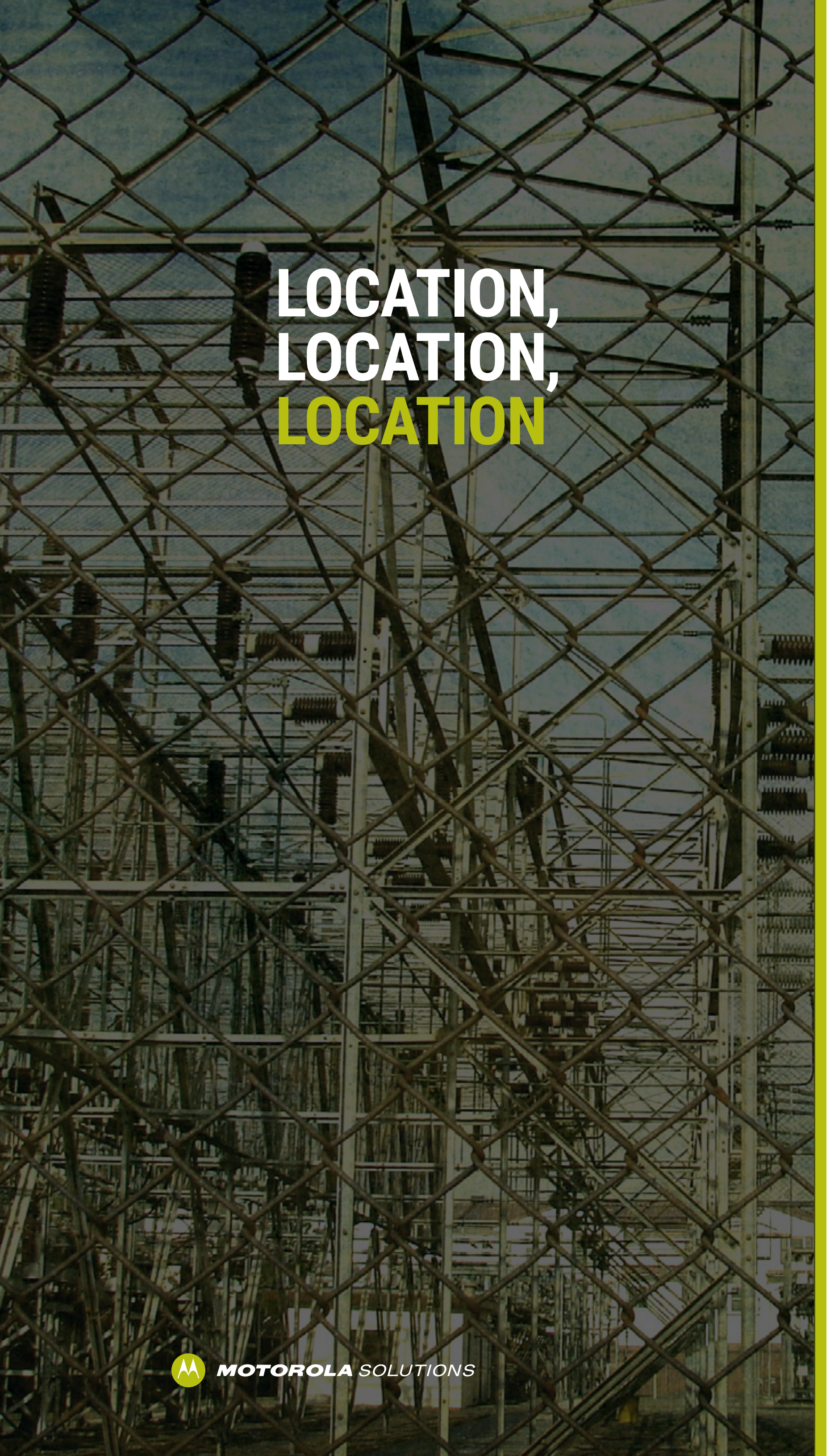
SUBSTATION DEFENSE BECOMES A UTILITY PRIORITY

Growing attacks on substations have triggered federal and state government responses. For example, just days after the Moore County outage the Federal Energy Regulatory Commission (FERC) directed the North American Electric Reliability Corporation (NERC) to review its existing physical security standard for the bulk power system and investigate whether the standard needs to be updated and improved. At the state level, legislators in North Carolina, South Carolina, and Arizona have proposed bills that would enhance substation security and make the penalties for damaging them more severe.

For utilities, there is obviously an urgency to adequately protect the substations that are needed to keep electricity flowing to customers. And the reality is that physical attacks on substations are just one of the threats utilities need to address. The rise of cyberattacks on energy infrastructure is also a growing concern, especially in the aftermath of the successful ransomware attack that shut down the Colonial Pipeline in 2021.

As the grid evolves to become more decentralized, digitized, and decarbonized, vulnerabilities are expanding. “All of this is compounded by the move to a smart grid,” said Mark Wantuck, a vice president at Motorola Solutions, who has decades of experience working with utilities to enhance infrastructure security. “The smart grid is getting the grid ready for EVs (electric vehicles), two-way power flows from renewables, and a lot more connected digital technologies that attackers look to exploit.”

Utility leaders aren’t wrong to be worried about cyber vulnerabilities. IBM released a report that identified energy as the third most targeted industry by cybercriminals, behind only financial services and manufacturing. The U.S. Department of Energy (DOE) painted a worrying picture of cyber concerns in its Multiyear Plan for Energy Sector Cybersecurity. “The frequency, scale, and sophistication of cyber threats have increased, and attacks have become easier to launch. Nation-states, criminals, and terrorists regularly probe energy systems to exploit cyber vulnerabilities in order to compromise, disrupt, or destroy energy systems.”



LOCATION, LOCATION, LOCATION

There are multiple challenges that make physical and cybersecurity at substations difficult. One has nothing to do with the unique vulnerabilities of individual substations. A challenge for utilities of all sizes is paying for the necessary defenses. “You’re always going to have budget issues,” said Chris Clark, a senior account manager with Motorola Solutions who also has decades of experience working with utilities. “Funds are always an issue because going out and doing a capital project and installing security systems can impact rates and you have to get approval from regulators.”

State legislation to enhance substation defenses could make utility investments easier by acknowledging the massive economic and societal disruption that occurs when substation attackers are successful in triggering an outage. But the regulatory process inevitably has tension between necessary investments to harden substations and the need to keep rates affordable for customers.

Beyond funding hurdles, the recipe for protecting substations from attack varies depending on their location. For example, many substations are built in rural areas, far from population centers. These sites generally don’t have any security personnel and only modest protections. “There’s probably a chain link fence and a gate and a chain with a padlock,” Wantuck said. “You can go out there and easily cut that fence or utilize equipment or tools to cause physical damage to the substation equipment.”

Substations located in densely populated urban areas have their own unique vulnerabilities. Urban violence and people painting graffiti on substation equipment are worries, even when there are plenty of onlookers. “A lot of these sites are protected more than the ones out in the middle of a cornfield,” Clark said. “But those in urban areas are still very vulnerable.”

PRIORITIZATION AND A COMPREHENSIVE DEFENSE

Not all substations are created equal when it comes to investing in their defense. Which is why one critical step to adequately protecting substations is to prioritize which infrastructure is most important to defend. In part, this is a function of compliance with NERC standards, particularly NERC CIP-014, which establishes requirements for the physical protection of critical transmission substations.

In fact, NERC CIP-014 requires utilities to identify which substations are most important to defend because of their impact on the reliability of the transmission system. That initial assessment triggers the development of a security plan to address specific risks at the substation and typically results in the implementation of security measures, including surveillance cameras, physical barriers, and personnel training. NERC CIP-014 also mandates regular compliance audits and assessments to ensure that the measures implemented are adequate to protect vital substations.

Not all substations are required to comply with NERC CIP-014. But utilities need to conduct a thorough assessment of all their substations to begin developing strategies to protect them from physical and cyberattacks. When Motorola Solutions' Wantuck works with utilities, he encourages on-site visits once utilities prioritize substation importance. "We'll start doing site walks with them. We'll identify what they feel is really at risk," Wantuck said. "And then we'll work with them to start designing the right solution."

THE FOUR PILLARS OF PHYSICAL SUBSTATION SECURITY

From the physical defense perspective, Motorola Solutions has a complete package of Safe Utilities tools that are built around four basic pillars of robust security: Detect, analyze, communicate, and respond. It's important to note that these pillars are interrelated and supported by an interoperable ecosystem of tools and technologies that deliver the visibility, understanding, and communication capabilities needed for utilities to protect all their substations.

Detection tools help utilities identify a security threat early, sometimes even before an attack occurs. For example, video cameras combined with analytics not only provides eyes to monitor activity around a substation but also intelligence to understand when a threat is acute. Indeed, Motorola Solutions can pair cameras with analytics that trigger alerts when a suspicious license plate or person is near or inside a substation's perimeter. "That's where license plate readers and other advanced technology come into play," Clark said. "We can load that information and the analytics can tell us this license plate was at three substations over the last month. Then we can look into it further to investigate what's going on."

Cameras and intelligence can be augmented by sensors that can pick up the sound of gunshots as well as ground-based radar that can detect if a drone is flying overhead. In some cases, detection can result in an automatic defensive response. "In rural areas, when there won't be any human security on-site, when a person is detected, spotlights can come on and a loud voice will say they're entering a sensitive area and need to leave," Wantuck said.

Whenever suspicious activity is detected, automatic alerts can be via text and text-to-voice directly to the radios and smartphones of utility staff responsible for response. As important as this is for effective deterrence and prevention of an attack, security footage and other information collected is helpful later for prosecuting criminals.

RESPONSE INFORMED BY ANALYTICS

While the detection enabled by security cameras, ground-based radar and other devices provide essential intelligence, analytics are what turn raw data into actionable insights. For example, video analytics allow security personnel to quickly identify a suspect at or near a substation based on their physical description, such as hair and clothing color. Mapping and GPS capabilities can also pinpoint the location of the security officer nearest to an intruder to facilitate a faster response.

Whether it's a high-priority CIP-014 substation with security staff always on-site or a remote substation defended only by a fence, communication is critical to effective substation security. Many utilities already have two-way communications solutions from Motorola Solutions as part of their emergency response strategy. Those solutions can be augmented with things like broadband capabilities that allow voice and data security information to be instantly shared with multiple devices in different locations. This can include sharing images of intruders attacking a substation. Improved communication also comes from automated alerts that keep dispersed security teams aware of an attacker's movements.

Detection, analysis, and communication are ultimately about maximizing the effectiveness of the fourth pillar of substation security: Response. Response can sometimes mean sharing information among utility security staff so they can assess a threat and decide whether to physically intervene. But it's also about coordinating with police and other public safety officials to share information about a fast-developing incident before they arrive at a substation.

ENHANCED SUBSTATION CYBERSECURITY

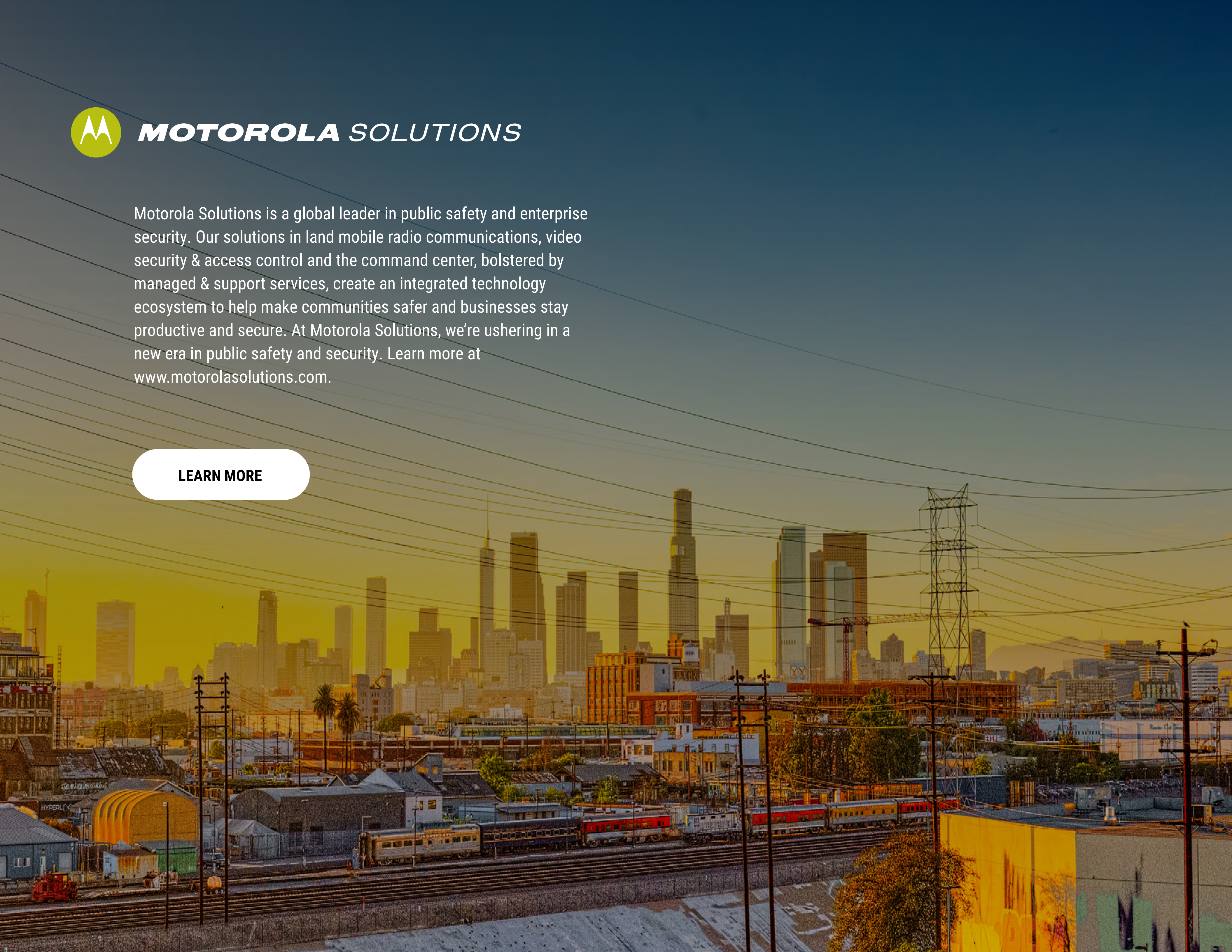
When physical attacks on substations lead to outages, the impacts quickly become well-known and public. But the reality is that substations, like the grid overall, are also vulnerable to cyberattacks that don't require an attacker to be anywhere near a substation.

Motorola Solutions' approach to substation cybersecurity mirrors its approach to physical security: it begins with identifying and protecting against risks, detecting when attacks take place, responding with a well-considered plan, and ultimately recovering from any attack and implementing changes to prevent future incursions.

Aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and NERC / CIP regulations, the Motorola Solutions Managed Detection Response (MDR) capabilities offer a robust and scalable cybersecurity platform that utilities can seamlessly adopt and implement. A full suite of cybersecurity solutions for critical infrastructure should include:

- Managed security services to protect endpoints, network, cloud and mission critical systems.
- Advisory or consulting services to identify vulnerabilities and develop a robust cybersecurity strategy with risk assessments, penetration testing and system recovery.
- Security patching capabilities to mitigate risk with pre-testing, validation and anti-malware software updates aligned to industry standards.

This holistic approach is best accomplished with an ongoing partnership that acknowledges that even the most sophisticated physical and cybersecurity defenses are of little use if people aren't trained to use the technology properly. "The most difficult part of the job is getting people to use the technology right, which means ongoing training and reinforcement," Wantuck said. "It's having somebody be there and educating them and helping them. When you make investments in security, you want to make sure you get the benefits."



MOTOROLA SOLUTIONS

Motorola Solutions is a global leader in public safety and enterprise security. Our solutions in land mobile radio communications, video security & access control and the command center, bolstered by managed & support services, create an integrated technology ecosystem to help make communities safer and businesses stay productive and secure. At Motorola Solutions, we're ushering in a new era in public safety and security. Learn more at www.motorolasolutions.com.

LEARN MORE

studio / ID

BY INDUSTRY DIVE

studioID is Industry Dive's global content studio, offering brands an ROI-rich toolkit: deep industry expertise, first-party audience insights, an editorial approach to brand storytelling and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

LEARN MORE