BURNS McDONNELL

WHITE PAPER / **UTILITY SECURITY ASSESSMENTS**

PROTECTING THE GRID TAKES A DELIBERATE TEAM APPROACH

BY Reed Galli, CPP

Gone are the days when the most significant security threat a utility faced was copper theft and vandalism. Today it's a different world. Protecting the grid against physical attacks and vulnerabilities is a big responsibility. Finding the right solutions — within budget — can be overwhelming. The answer lies in a strategic formula and collaborative approach among security professionals, public relations specialists and engineers.

The 2013 attack on the Pacific Gas & Electric Metcalf Substation was a dramatic event that exposed the vulnerability of the electric grid. Ever since, utilities have been confronting this new world of increasingly dynamic threats.

With the creation of the NERC CIP-014 standards in response to this new threat environment, proactive tactics are necessary at both regulated and company-critical sites. These regulations are leading some utilities to the establishment of security measures to deter, detect, delay and respond to threats as complex as snipers or car bombs. These measures can be multifaceted and require professional assessment and implementation. It's not just a fence surrounding a substation. It's permitting and grounding a 14-foot climb- and cut-resistant, ballistic-rated fence with fence-mounted intrusion detection systems — and making sure the neighbors understand why with clear and consistent reasoning.

SEEING THE CHALLENGE FROM BOTH SIDES

As a physical security specialist for a large utility, I saw firsthand the unique challenges associated with protecting control centers, substations and critical assets. Often, our team was so engulfed in day-to-day security tasks it was difficult to address big-picture issues. We knew the details of our utility's specific infrastructure and procedures better than anyone, but the time and staffing to identify unique solutions for critical asset protection was minimal.

My career has now transitioned into the consulting world, helping electric utilities in North America meet physical security regulations and improve overall security operations. With that transition, I now have the advantage of using my rich experience to develop and implement a deliberate approach that provides a road map to achieving security objectives for many utilities.

The formula is straightforward and practical: A laser focus on the basic security principles of risk assessment, site-specific planning and a holistic design approach.

RISK ASSESSMENT

Taking the next step to risk assessment is what helps justify allocated resources. Mary Lynn Garcia, a Sandia National Laboratories principal and author of several books on physical security, says the goal of the risk assessment is to help decision-makers prudently spend their budget to most effectively reduce security risk to their facility.

Fences, video surveillance, electronic access control, vehicle barriers and intrusion detection systems can take a big bite out of a utility's security budget. With larger expenditures come questions about value. The ability to quantify mitigation measures is vital for justifying resources to auditors, senior management and even public service commissions.

Tools such as CARVER (Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognizability) and RAM (Risk Assessment Methodology), among others, can provide a risk estimation value for each threat or mode of attack. This value is derived from formulas using the probability of a successful attack based on changing vulnerabilities, impact and the ability to recover. There isn't necessarily a right or wrong methodology. The constantly shifting nature of event probabilities can necessitate security strategies that adapt to a dynamic threat environment.

SITE-SPECIFIC PLANNING

Once a risk estimation value is assigned for each threat, the next step is creating a mitigation plan that the community will accept and that can be permitted in a timely manner. The most effective solution is implemented in a layered approach, with the first detection zone at the greatest distance from the critical asset. An adversary should face multiple layers of security to increase the probability of detection and allow more time for law enforcement and/or security officers to respond before an event becomes critical.

In a Metcalf-style attack, for example, a shooter outside the perimeter fence should face an intrusion detection system (gunshot detection and/or ground-based radar) at the line of sight to the critical asset. This example leads to another basic principle: Site-specific planning.

Each site has distinctive characteristics that need careful examination and analysis. Substation design engineers and security specialists have a lot to consider, from elevation to vegetation.

Some site characteristics are obstacles that an adversary would have to overcome, such as tree lines that act as a barrier by blocking the line of sight to critical high-voltage transformers. Others can be assets, such as cell towers that offer greater height (and thus better performance) for wireless routers and surveillance cameras.

After assessing the risk and examining unique site characteristics, a detailed design plan must be drawn up. When I worked for a utility, I often saw this step addressed with a rough sketch or delegated to the contractor installing the equipment (see "Cautionary Note" below).

In retrospect, I see the consequences of giving this important step insufficient attention and have developed a greater appreciation for detailed drawings and specifications. Thorough plans take the guesswork out of what, where and how security devices are installed.

A SAMPLING OF SITE-SPECIFIC FEATURES THAT IMPACT SECURITY SYSTEMS

- Adjacent property owners
- Culverts
- Elevation
- Landscaping
- Lines of ingress and egress
- Location of tree lines
- Natural barriers
- Nearby cell towers
- Nearby railroad tracks
- Types of roadways/driveways
- Types of vegetation
- Water drainage outlets

DETAILS MAKE THE DIFFERENCE — A CAUTIONARY NOTE

"A simple sketch is sufficient, right? After all, the installer knows what to do." Sometimes it's more complicated, as this fictional but plausible story illustrates.

- A technician in the field is pulling Cat 5 cable for a camera. Without a detailed sketch to provide clear direction on the cable path, the installer does his best.
- A few weeks later, an IT technician troubleshooting network issues notices an unfamiliar Cat 5 cable and traces it to a network switch. The cable has no markings, so the technician disconnects it, thinking it's extraneous or was used for troubleshooting.
- Soon, a security officer notices and reports the offline camera to a supervisor, who contacts the security contractor.
- A technician — perhaps one unfamiliar with the facility — arrives to troubleshoot. Discovering no problems with the camera, he notices the cable isn't plugged into a network switch. Without drawings to reference, the technician chooses any open port on the closest network switch.
- The technician calls the security operation center to verify the camera is online. It's not, so the technician requests a network engineer to verify the port is activated. The network engineer isn't able to remotely activate the port right away, so the technician makes a second service call to reprogram the camera's IP address.
- The cost to "repair" the disconnected camera is almost equal to its original price.

It sounds like a comedy of errors, but in reality this isn't an unusual circumstance. Drawings that specify the camera, cable run, network switch and assigned data port, and communications between departments, could make all the difference.

A HOLISTIC SECURITY APPROACH

Potential threats to critical infrastructure are growing more diverse and sophisticated, and a utility must be prepared. A holistic security approach is fundamental to the prudent and compliant operation of these critical assets.

Security is more than hardware; policies and procedures have a tremendous impact on operations. With the new NERC CIP-014 requirements, many utilities are installing electronic access control at gates into the switchyard. Employees must have a keycard to gain access. But what happens at 3 a.m. on a weekend when the substation electrician doesn't have his card and needs access to respond to an outage?

It's vital for employees to gain access to critical equipment, as every second of delay affects power restoration efforts, reliability indices and customer satisfaction. But physical security is also a priority, so a plan must be in place to balance both needs. Electronic access control systems, doors and electric locks should also address abnormal operations.

Employees (and contractors) must also understand why the company is investing in security. I'm sometimes surprised at how many utility employees with responsibilities inside switchyards are unaware of the Metcalf incident and CIP-014. Without a clear understanding of what's driving these changes, they might consider a "Big Brother" scenario or not be able to clearly and consistently address neighbor or customer questions and concerns. With understanding, a sense of ownership can be instilled as employees become part of the security solution.

Security awareness training is an excellent idea for these situations. Explaining the reasoning behind the investment and outlining their role in reporting suspicious activity helps create a sense of responsibility and teamwork for security. Time invested in training is well spent.

BRIDGING THE COMMUNICATION GAP

Electric utilities are undergoing the tedious and necessary process of identifying and protecting critical assets to meet regulations. The CIP-014 standard is bringing together utility departments that may not have interacted before. And while a utility's transmission engineers and security managers share a common goal, they may approach the situation in completely different ways.

Having been a client and a consultant, I've seen firsthand that need for a diverse skill set. Our team offers deep experience in both substation engineering and physical security. On one hand, we can help explain permitting and installation changes for a cut- and climb-resistant security fence that can cost hundreds of dollars per foot. We can also discuss the pros and cons of video surveillance on the SCADA system with IT personnel and deliver detailed drawings and specifications of proposed security devices.

Advances in physical security technology are rapidly coming to market. With limited staff and resources, corporate security departments often don't have the internal resources to stay ahead. It's our priority to maintain the necessary skill set, with more than 80 substation security assessment and recommendation projects in our portfolio. Being independent and not associated with specific manufacturers or integrators, our only responsibility is to a utility's security objectives.

The adversary is able to adapt faster than regulations can keep up. Being proactive is the best method of mitigating these threats. Protecting our infrastructure from intentional harm is a tough job — and it requires a true team effort.

BIOGRAPHY

REED GALLI, CPP, is a senior physical security specialist for Burns & McDonnell. He has more than 14 years of experience in physical security consulting from both the private and public sectors. Reed has extensive experience in electronic security deployments, including electronic access control, intrusion detection systems and video surveillance. He also has project management experience for security installations in a variety of facilities, including electric utility substations, data centers, higher education, athletic stadiums, libraries, research labs, call centers and Class A office buildings.

11968-PTG-0916