Coal Plant Shutdowns: Operators Have Cyber Protection Obligations Even After Closing

Related People:
J. Wylie Donald

Environment & Energy Alert

08.29.2016

As Yogi Berra used to say: “It ain’t over till it’s over.” Coal plant operators shutting down their plants should remember this phrase. Even after they throw the breakers, go off the grid, are no longer contributing to the bulk power system, and begin to take apart their plant, operators still have cyber protection obligations under the North American Electric Reliability Corporation (NERC) Reliability Standards and state and federal data security laws.

Cyber Risk

More than a decade ago, before the NERC Reliability Standards were approved, one large generator in the Northwest got into trouble when it sold 230 hard drives to a salvage company. The salvage company turned around and sold a third of the drives on eBay. One of the purchasers was a university IT director, who was able to recover grid diagrams; confidential law department data concerning lawsuits, contracts and transactions; and employee information, including Social Security numbers.

The Reliability Standards have made this kind of potential cyber catastrophe very rare. A review of NERC’s enforcement records discloses temporary loss of control of only single pieces of equipment with cyber information still intact. Still, all it takes is one error. As one of the NERC regional entities stated in an enforcement proceeding, “Failure to establish controls to dispose of Cyber Assets could allow malicious access to sensitive information related to cyber security or reliability. Such information could then be used to get access to Critical Cyber Assets essential to the operation of BPS [the bulk power system] and potentially disrupt the operation of the BPS.”

Operational Assets and Shutdown

NERC regulation of cyber assets extends beyond the time the plant is providing power to the grid. Utilities decommissioning cyber assets must “take action to prevent the unauthorized retrieval of [bulk electric system] Cyber System Information from Cyber Asset data storage media” prior to disposal or redeployment (CIP-011-2). That is, any electronic storage media (e.g., hard drives, random access memory (RAM) or read-only memory (ROM), optical storage, flash drives, or backup tapes) must be properly sanitized.

The NERC obligations extend beyond addressing the decommissioned device. Operators must also ensure that holes are not opened up in the cyber systems that remain and that documentation is appropriately maintained. Among other obligations, a failure to update firewall settings may lead to firewall ports remaining open when they should be closed (CIP-005-1 R2). The decommissioned assets must be considered in the entity’s cyber vulnerability assessment (CIP-005-3a R1). Electronic security perimeter diagrams must be updated to reflect the withdrawal of

the cyber assets (CIP-005-3a, R5). Operators are required to report changes to their baseline control system configurations (CIP-010-2).

But the operator is taking apart the plant; surely, NERC compliance obligations must end? They do. NERC's compliance registry must be updated. One process wrinkle is that NERC adds and omits entities from the registry on an organizational basis. This does not comport with circumstances where the organization is eliminating a generation asset but will continue to operate other NERC-subject assets. Fortunately, the NERC regional entities keep track of assets via "asset verification" forms, and many expressly require notification of changes to a Registered Entity's asset portfolio. The bottom line: Keep NERC informed.

Personal Information

A plant's cyber responsibilities do not end with NERC. If the plant keeps personal information, which can be broadly defined depending on the jurisdiction, then state and federal requirements will also apply to the disposal of media containing that information. For a coal plant, two sets of rules are paramount: first, rules governing "consumer reports" enforced by the Federal Trade Commission (FTC), and second, rules governing personal privacy and data security enforced by individual states.

The FTC enforces various laws directed at protecting consumers. Potentially relevant to a coal plant is the Fair and Accurate Credit Transactions Act (FACTA), which requires the proper disposal of customer information derived from "consumer reports" obtained for a business purpose. Any business that obtains a credit check on a consumer or a background check on an employee—*i.e.*, a "consumer report" as defined by the statute—is subject to the rule. The FTC's "Disposal Rule" mandates the proper disposal of such information through "reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." For electronic media, those reasonable measures may include destroying or erasing the media so that the regulated information cannot be read or reconstructed and conducting due diligence on the media disposal vendor.

Besides enforcement under the Disposal Rule, the FTC may also bring enforcement actions under Section 5 of the Federal Trade Commission Act, which prohibits "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." The Commission's authority to pursue businesses that fail to protect their customers' personal information was upheld last year when the FTC prevailed in *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015). As the FTC proclaims on its website: "The decision is a must-read for business executives and attorneys."

Utilities, to our knowledge, have not yet found themselves in the FTC's sights. Others have not been so lucky. The FTC regularly pursues entities that through theft or other means lose laptops containing personal information. Dumping records containing personal information in dumpsters will bring unwanted FTC attention. The FTC settled a claim against a student loan provider that failed to erase old hard drives it sold to the general public.

Where FTC jurisdiction ends, state jurisdiction takes over. Almost every state has a data privacy and security law that applies to businesses handling regulated personal information, which may be broadly or narrowly defined. Such laws typically specify who has the compliance obligation, define the scope of "personal information," and outline what constitutes a breach and the timing and method required to give notice of the breach. For example, Illinois requires that the disposal of regulated personal information render the personal information "unreadable, unusable, and undecipherable." 815 ILCS 530/40(b). In Colorado a company is in violation if there is "unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity." Colo. Rev. Stat. § 6-1-716(1)(a), (2).

Besides government regulatory action, data breaches also breed lawsuits. Whether the plaintiffs are customers annoyed that their credit cards numbers are being pilfered, a shareholder irate over the drop in stock price, or an employee upset over his identity being stolen, companies involved in data breaches often find themselves defending lawsuits.

The takeaway is that cyber information exists at coal plants and is subject to regulatory obligations regardless of the operational status of the plant. Further, the time to focus on the disposal of cyber assets is at the beginning of the process, when the mindset of management and the involved individuals is still the mindset of people operating a plant. If equipment and media hang around for a year or more, the razor-sharp cyber protection protocols used during operation will have inevitably dulled.