ZIMPERIUM

NERC CIP & Mobile Devices

The Facts About Mobile Security & Compliance

Fact #1: NERC CIP has included mobile since it took effect in 2008

By now, any IT professional working in the utility industry should be familiar with NERC CIP. The requirements are designed to secure the assets required for operating North America's electricity grid and specify the minimum that must be done to protect bulk power systems. Any entity operating such power systems in the United States, Canada and a part of Baja California in Mexico must comply with NERC CIP.

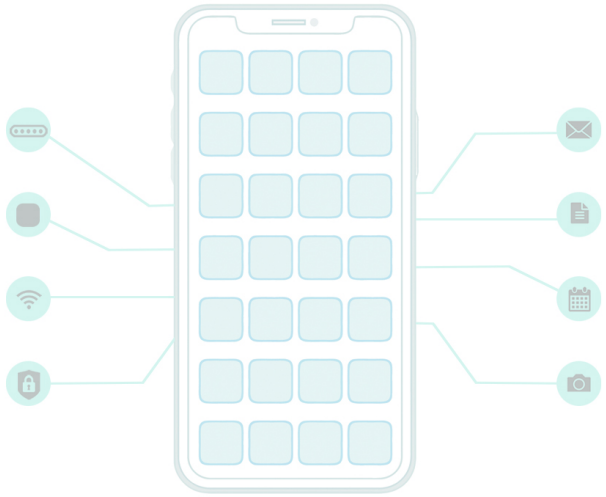
What may not be as widely known is that NERC CIP requirements have applied in principal to mobile devices ever since FERC approved the first version of NERC CIP in January, 2008. In February of the following year, the DOE published a paper observing that "CIP compliance is challenged when mobile devices ... are able to access a CIP-protected cyber asset within the ESP. **... Cell phones and pagers are prime examples."**

In other words, if your NERC CIP compliance measures do not yet include mobile devices, you are out of compliance.

Fact #2: Mobile devices are 60% of NERC CIP-covered endpoints

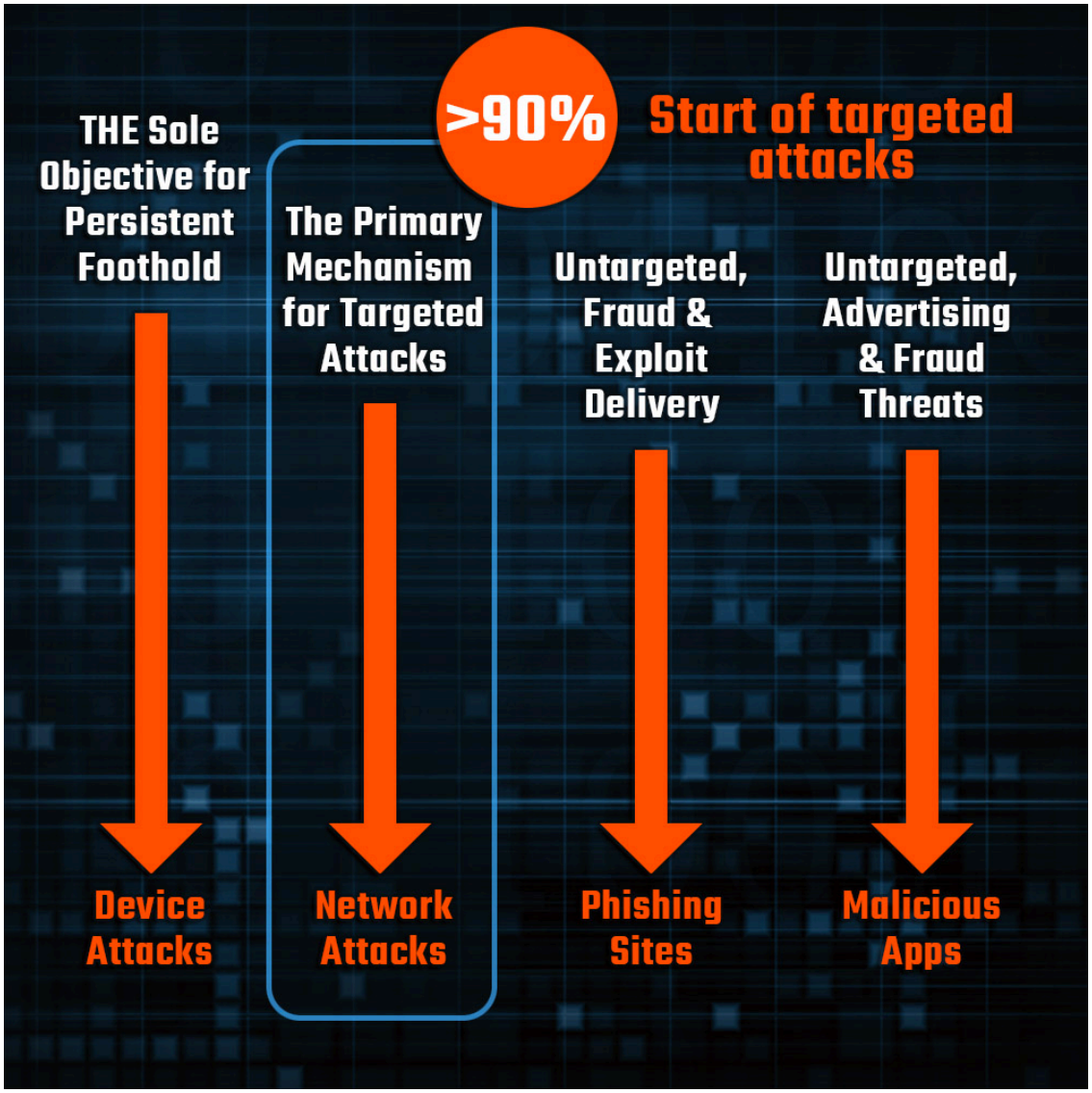
NERC CIP noncompliance has been declining since 2014 as organizations subject to NERC CIP have invested significant resources toward achieving compliance. The problem arises when utilities focus on protecting endpoints without realizing that **mobile devices are endpoints**, both with respect to NERC and in general.

Mobile devices are in increasingly wide use as a platform for productivity in the energy sector. That means that the traditional computing devices (e.g., servers, desktops and laptops) that utilities have focused their security and compliance efforts on are only about 40% of their total endpoints. The other 60% of devices that connect to your network—mobile devices—must be made NERC-compliant as well.



Fact #3: Mobile endpoints are under attack

One critical difference between mobile devices and other types of endpoints is the variety of attack vectors that mobile devices are exposed to. Ensuring the integrity of mobile devices requires protecting them against all of these forms of attack.



Fact #4: Mobile requirements for mobile are explicit

Zimperium helps you meet the mobile mandates for the NERC CIP below.

SECTION	SUBSECTION	PROVISION
CIP-007-6	R2	**Security Patch Management**
	2.1	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets.
	2.2	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.
CIP-007-6	R3	**Malicious Code Prevention**
	3.1	Deploy method(s) to deter, detect, or prevent malicious code.
	3.2	Mitigate the threat of detected malicious code.
	3.2	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.
CIP-007-6	R4	**Security Event Monitoring**
	4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:
	4.1.3	Detected malicious code.
	4.2	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):
	4.2.1	Detected malicious code from Part 4.1
	4.3	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional

Fact #5: Zimperium is the solution for mobile NERC CIP compliance

Zimperium leverages a patented engine to detect mobile device, network, phishing and app attacks in real time. The engine runs efficiently on smartphones and tablets without violating user privacy. To date, the engine has detected 100 percent of zero-day device exploits without requiring an update or suffering from the delays and limitations of cloud-based detection or legacy security architectures, making Zimperium uniquely capable of meeting NERC mobile requirements.

Contact Zimperium for NERC CIP mobile compliance

When you are ready to ensure compliance with NERC mobile requirements, please contact us for a custom evaluation.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244