Are You Prepared to Respond?

Even the best protective measures can't guarantee that you won't suffer a cyber security event. So, no security program is complete without detailed recovery plans. In fact, they make up an essential part of the NERC cyber security standards (CIP-002 through CIP-009). These require Bulk Electric System (BES) companies to define, document, and test measures to restore and resume operation of every critical cyber asset in their inventory.

Most Responsible Entities have emergency procedures to address NERC EOP-008. These maintain reliability operations if their primary control center becomes inoperable. However, the CIP-009-1 requirements tackle an entirely different goal – the full recovery of cyber assets after an event. This can range from correction of a simple account use violation to restoration following a major network attack that disables workstation and server computers across the organization. Moreover, the standard re- quires plans for critical cyber assets outside the confines of the control center – for example, in a substation or a generation plant.

Too Many Eggs in One Basket

When a disabling incident occurs, most companies rely on a small team of key individuals to identify and fix the problem. They assume these personnel have intimate knowledge of the system's hardware and software that enables them to bring it back on line quickly. So, what happens when one or more members of the team are unavailable?

In the NFL, most teams have their star player. They rely on this individual to make the big play and win the game. Often he does. Sometimes he doesn't. But, unlike the NFL, you can't afford to lose when you have a failure of one of your critical cyber assets. And, while that football team may have its star, it has a well-rehearsed game plan that involves every member of the squad – complete with a capable coaching staff to coordinate.

Preparedness is the key.

When an event occurs, there's no time to design a new system. Your organization can't wait for delivery of key equipment or media from the manufacturer. Most importantly, you can't afford delays and downtime due to a forgotten step or misplaced priority. The response must consist of a well-organized and documented process that brings up each component of the EMS or other critical cyber asset in a pre-defined sequence. You and your team must know each step before it's taken. Coordination and execution of the recovery procedures should not lie in the hands of a single individual.

NERC CIP-009 RECOVERY PLANS

Voice (845) 620-9500 Fax (845) 512-2093
http://www.netsectech.com

NERC CIP-009 RECOVERY PLANS

Strategy vs. Tactics

Just as a football coach studies his opponent before the game, you must understand all the threats and impacts you face when planning your cyber asset recovery process. After all, using a passing defense against a running offense makes no sense. Your plan must consider a variety of scenarios, such as:

- Accidental or intentional changes to authorized cyber asset accounts or privileges,
- Accidental or intentional deletion or modification of critical reliability data and databases,
- Disablement of EMS applications, operating systems, security components, device configurations, or IED firmware,
- Physical destruction of equipment through direct or indirect means,
- Infection of workstations, servers, and other cyber assets by a computer worm, virus, or Trojan Horse,
- Network attacks such as distributed denial of service, flooding, route manipulation, or DNS cache poisoning.

Execution makes up the other half of the equation. A good coach knows that his team must have the plays to enable them move the ball down the field. So, too, your organization must possess the tools to address any scenario. For every critical cyber asset, your plan must detail the steps to:

- Establish temporary alternate measures for essential reliability operations.
- Contain and eliminate the cause of the initial problem.
- Procure or allocate the systems and other necessary materials.
- Install equipment, software, and other components to restore baseline function.
- Load the configuration, operational data, and databases.
- Test and cut over to production operations.
- Remove temporary measures and re-establish preparedness profiles.

Does your recovery plan include all of these? Does your documentation provide up-to-date information to recover operations, even if key personnel are absent? Can managers understand and coordinate the team's activities? Can your organization pass a NERC CIP- 009 audit?

Our Team Can Help Your Team

Network & Security Technologies, Inc. (N&ST) has the know-how to create an effective recovery plan. We develop and document procedures for reliability operations in all aspects of the Bulk Electric System. These include hands on experience with most North American Energy Management Systems (EMS) as well as a wide variety of RTUs, relays, IEDs, and network devices used for substations and generation plants.

Our consultants won't spend their time learning about your hardware or software. Instead, we will document a game plan tailored to your operational configuration. This consists of the information you need to coordinate recovery of critical cyber assets, guide technical and other team members, and maintain your plan through regular drills and exercises. Our final product helps to ensure full compliance with NERC CIP-009-1. It will enable a complete recovery without reliance on key individuals and give you the peace of mind that you can restore normal reliability operations in the face of any cyber outage.

Network &Security Technologies

161 North Middletown Road, Pearl River, NY. 10965

Our passion for technical excellence and commitment to our client's business success results in practical solutions to complex problems