NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

ICCP Communication Failure Due to Firewall Patch Update

Primary Interest Groups
Reliability Coordinators (RCs)
Balancing Authorities (BAs)
Transmission Service Providers (TSPs)
Generator Owners (GOs)
Generator Operators (GOPs)
Transmission Owners (TOs)
Transmission Operators (TOPs)

Problem Statement
During a regularly scheduled firewall patch installation, a TO (hereafter, the "entity") experienced multiple inter-control center communications protocol (ICCP) communication failures with external entities.

Details
The entity, with the support of on-site contracted services, performed a patch update to its main control center (MCC) ICCP firewall. This resulted in an outage of ICCP communications for greater than 30 minutes, constituting a reportable event per EOP-004.

The entity has two fully redundant computer systems that it uses to operate and maintain its transmission system. The network security team has the ability to relocate system operations remotely so it typically applies patch updates at the MCC after the transition to the back-up control center (BCC). Once the transition has occurred, the patch is then applied to the primary system and tested before it is applied to the backup system. The network security team then tests the systems by swapping between them.

Per its testing process, the entity transferred its ICCP communications from its MCC firewall to its BCC firewall to install a security patch on the MCC ICCP firewall. Once the patch had been tested on the MCC, the system was transferred to the BCC, where it caused multiple ICCP communication failures with external groups. In addition, the patch prevented the network security team from being able to transfer the system back to the BCC remotely, and so the team needed to physically travel to the BCC to bring the unpatched system back on-line and restore the ICCP connectivity. This delay caused the duration of the ICCP outage to be greater than 30 minutes.

During troubleshooting of the issue, the BA's electronic dispatch system (EDS) intermittently failed, and the entity's system operator requested that all generating units they were responsible for dispatching be placed on verbal dispatch. Throughout this event, the entity's system operators maintained control of their system and could shed load, and both the energy management system (EMS) state estimator (SE) and the real-time contingency analysis (RTCA) tool continued to solve.

The entity was not able to bring its redundant MCC ICCP connectivity in service until the following evening. The entity determined that the best way to approach the issues was to remove the patch and return its MCC firewall to its original configuration prior to the event before restoring it to normal operation.

An internal investigation was performed that identified the following key contributing factors for this event:

- The assets being updated were identified as CIP "qualifying" assets and were not considered CIP "critical cyber assets" (CCA) per the CIP Standards. The entity's change control process for a qualifying asset did not require advance formal notifications and reviews from all possible stakeholders that would be required for an identified "CCA" asset. The security team adhered to its change control process and communicated the work being performed just prior to the transferring of systems. The late communication is believed to have contributed to the severity of the event and its duration.
- Just prior to this scheduled firewall patch update, the entity had installed a network upgrade that supports its EMS system. The entity relied upon the on-site contractor's expertise of the new equipment to assist with the patch update and to determine any possible impacts to the system.
- The entity's network security team and contracted resource communicated the change just prior to implementation. The entity believed that the patch update would not have any negative operational impact and therefore did not communicate with enough time and detail such that the EMS/Operations/IT staff could identify any potential risks and mitigate them.
- While the entity does have two separate redundant systems that it uses to support its control centers, it does not have a full, off-line replicated network test system. An off-line test system and rigorous testing procedures might have identified some or all potential update problems/symptoms without a risk to the production system. Testing on the MCC while the BCC is in control reduces risks, though the two systems still have some degree of interaction that can cause adverse impacts, as was experienced here.
- Due to the timing of the newly installed equipment and the patch update, all of the formal work instructions had not been completed prior to the initiation of this work. With the contractor on-site, the entity believed that their expertise could allow them to proceed with the patch upgrade.
- In addition, due to building construction, the working environment during the event was not ideal for this type of critical work. The network/IT department did not have full visibility of overall system performance due to its location during the event; if they had it, it is likely they would have minimized the severity and duration of the event. The entity has since completed construction, and all critical work is now performed within a location adjacent to both the EMS and Operations department. This should increase communications, awareness, and response times going forward.

Corrective Actions

The entity recommended these steps to address the issues that led to this event:

- Develop an overarching, formal governance program for work being performed within the Network/IT department. This includes the development of specific procedures/plans for all work performed on devices that can significantly impact the operation of the system and not only for those identified as "CCA." The devices for the purpose of this investigation are devices that could

impact any of the services provided by the network systems. Multiple actions were identified by the entity and are listed below:

  - Define, identify, and document devices that can have significant impacts on the operation of the system beyond CIP compliance.
  - Review, revise, and improve the change management processes/work flow/program/work instructions with defined devices. This will include communication of information regarding scheduled work, quality control, work oversight, risk evaluations, and resource scheduling.
  - Develop work instructions for implementing and upgrading the identified devices (e.g., test backup systems on a regularly scheduled basis and perform device imaging prior to updates).
  - Communicate with the Operations Department whenever work is scheduled on systems which could have an impact on the EMS/SCADA or ICCP systems.
- Continue to enhance the entity's approach to working on complex network systems with no replicated off-line test system.
- Develop work environment norms and tools to facilitate critical work activities.
- Continued Analysis:
  - The entities system was restored to a tested and proven state. The system is not directly attached to the Internet, and the entity still maintains a defense-in-depth posture to ensure operations continue in a safe and risk adverse manner.
  - The entity continues to work with the vendor of the security patch. The goal is to replicate, as close as possible, the production environment in the vendor's lab. The entity needs to ensure the validation of the upgrade process moving forward, and if possible, identify the functionality change that contributed to the ICCP communications failure.

Lesson Learned

- Network/IT work plans and priorities should be identified with enough time to fully vet any concerns or impacts a security patch could possibly have on the system and involve all possible stakeholders in the planning.
- Entities should identify and define devices that can have a significant impact on the operation of the system beyond the CIP standards. This will make certain that this type of work is vetted well and communicated to all stakeholders.
- Early communication of all work being conducted, whether deemed to be low or no risk to the system, should always be shared between departments.
- Create a work environment that is conducive to the complex work being performed. This environment should have access to both the EMS and Operations departments while this work is being performed. In addition, entities should create working norms for employees within the work environment to prevent distractions or interruptions (e.g., create a means of communication with stakeholders while work is being performed).

- Identify the worst case scenario(s) that could occur from your companies patch update processes. Develop a plan that would mitigate these risks and identify the key actions that can be taken to minimize the risk to the system and duration of the event if the worst does happen.

NERC's goal with publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC requests that you provide input on this lesson learned by taking the short survey provided in the link below.

Click here for: Lesson Learned Comment Form

For more Information please contact:

NERC – Lessons Learned (via email)	NPCC – Event Analysis
Source of Lesson Learned:	Northeast Power Coordinating Council
Lesson Learned #:	20160604
Date Published:	June 14, 2016
Category:	Communications

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.