Cyber Security Response to Physical Security Breaches

INTRODUCTION

Physical break-ins and other unauthorized entries into critical infrastructure locations, such as electrical power substations, have historically been viewed as traditional property crimes where trespass, theft, and vandalism were the motives. However, the current trend of using computer networks to remotely monitor and control unmanned facilities has also increased the possibility that these physical property crimes could be used to conceal less discernible cyber crimes. For example, the physical breach of an electrical substation to steal materials and equipment could be viewed as a simple case of burglary. In the current environment however, such an event could just as easily be a distraction to draw the asset owner's attention and investigation away from the real motive. What if the underlying motive was to gain access to the systems and devices within the facility in order to either launch an immediate cyber attack? Or, introduce hardware or malicious software into the control system network, thereby establishing a cyber foothold for future attacks or stealing sensitive information?

SECURITY IDEALS

The following information details a cyber security response that critical asset security managers can implement to determine if a cyber asset was targeted during a physical breach. A systematic series of suggested actions or checks is provided to assist in judging the integrity of cyber-based equipment as well as determine if a cyber security incident has occurred. These are only suggestions, and should be considered within the existing operational reliability, procedures, and safety policies of the owners and operators.

This document does not prescribe a process for investigating criminal activities, nor is it intended to conflict with any official investigation requiring specific procedures for collection, analysis, or preservation of evidence for criminal prosecution. Rigid state and federal rules of evidence can vary significantly from even the most prudent commercial procedures and practices.

SCENARIO

The actions, checks, and other suggestions prescribed herein could apply to virtually any remote, unmanned facility where cyber-based control systems are employed. However, for simplicity sake, the scenario in this document deals exclusively with a physical security breach of an unmanned electrical substation. In this scenario, an electric power substation has been broken into and an investigation is underway by the owner/operator security manager in accordance with applicable corporate policies and procedures. An inventory and damage assessment is being conducted with care so as not to contaminate the scene or damage evidence in the event local law enforcement is brought in to conduct a criminal investigation.

Indications of a physical security breach may include, but are not limited to:

- unauthorized door alarms
- unauthorized personnel recorded on a substation video camera (if installed)
- damage to door lock or outside barrier fence
- evidence of vehicles or persons outside and inside the fence (tracks in the dirt or impressions found in the gravel typically used in substations)
- loss of communications that cannot be explained by the communications provider
- unexplained or anomalous behavior exhibited by control system devices
- missing or unaccounted for items

Those investigating a physical security breach should be aware that a cyber related incident may also have occurred. If the investigation of a physical security incident reveals that cyber assets have been impacted, the actions in the following sections may be implemented. It is recognized that electrical substations are operational assets at risk with economic, regulatory, and safety consequences. Any unauthorized changes to a control system's configuration or software have the potential to significantly impact asset availability and safety, thereby producing potentially unknown risks to its operation and indirect risks to customer organizations.

ASSUMPTIONS

When a physical security breach occurs at an electrical substation, the asset owner must be properly prepared to validate the availability and integrity of all cyber assets (as defined in NERC CIP-002-1). The extent of the investigation will depend on indications discovered by the asset owner in and around the area where the physical breach occurred. The actions presented take the following assumptions into account relating to the electrical substation:

- Network connectivity exists inside the substation or between another substation/control center and the affected substation.
- Electronic devices with the capability to obtain, store, or transmit electronic data exist in or around the electrical substation.
- Devices (wireless devices, modems, Ethernet switches, PSTN, fiber, programmable logic controllers, and intelligent electronic devices [IEDs]) exist at the substation that perform control and network functions.

For the purposes of this paper, a cyber security breach is defined as an unauthorized network intrusion or an unauthorized physical connection to a computer system or network device.

ESCALATING AN INVESTIGATION

A systematic series of checks can be conducted to help determine if there is sufficient evidence to indicate that a cyber security breach may have occurred in conjunction with the physical breach. The escalation of the levels of examination provides a process to judge the risk of a cyber intrusion with increasing levels of information, but it also increases the impact to system operations.

Three levels of examination are considered: initial examination, system checks, and a detailed examination of file systems and binaries. Each level of escalation is more invasive and thus requires more expertise and coordination with the facility or organizations responsible for cyber security and production operations. Management must be able to assess and balance the risks of escalation with the potential for outages along with equipment and personnel safety risks caused by a cyber intrusion of a critical asset. If the escalation of an investigation into a possible intrusion continues, it is likely that any significant tests on control components will require specific test plans, procedures, and perhaps scheduled outages to obtain the necessary information.

Before cyber assets are examined, an individual familiar with the area where the intrusion occurred must examine the area for anything that appears out of place (this practice is usually referred to as a “yard or station walk down”). A staff member who is familiar with the control devices and connections at the substation should also be present to examine the scene. It is important to log all observations. Photographic or digital video records of any physical evidence can also be very helpful. What may not seem significant during the initial discovery can prove significant as the investigation proceeds. Again, care must be taken to preserve evidence in case the asset owner elects to involve its local law enforcement agency.

Escalation beyond the initial examination described below requires actions and expertise commensurate with that required for installation, upgrades, or restoration of service of the control equipment by the appropriate vendors, consultants, or corporate support organizations. Management should determine if it is necessary to pursue any forensic analysis in support of law enforcement investigations and to identify and direct appropriate expertise in providing that support.

If law enforcement is brought into facilities to conduct an investigation, facility management should provide a briefing on the “do’s and don’ts” regarding any of their actions that could affect its operational status. The facility security manager and/or operations staff should be present to ensure that operational and personnel safety procedures are followed.

NOTE: *The following checks are only suggestions and should be implemented based on the installation’s cyber assets.*

1. INITIAL EXAMINATION

The first step is to examine items that can be checked visually. The use of digital photography with a date and time stamp is critical for documenting potential evidence. Visually examining items can include the following:

- Look for signs of entry into the building or cabinets where cyber assets are stored. This could include footprints or disturbed items inside and outside the building.
- Look for evidence of tampering with all cyber assets. For example, disturbed dust or dust texture and composition inconsistent with that around it, broken tamper seals, or signs that a rack or case has been opened. Coordinate with your local law enforcement, as they may also be interested in obtaining forensic images of the compromised systems.
- Check physical connections to all cyber devices such as network devices, and other equipment intelligent electronic devices (IEDs).

- Check front panel indicator lights for proper illumination; compare to station checks (normal illumination).
- Check for missing or new unknown hardware located in and around the substation. This includes checking telecommunications equipment that might be outside the perimeter. For example, there are several commercially available hardware and software-based keystroke loggers that are difficult to detect.
- Check with the control center to see if any unusual alarms, events, or logs appeared on the control system, or if any breaches of connectivity or service occurred during the timeframe of the intrusion.
- Analyze the physical breach to determine a motive and correlate it to any cyber information or devices. Does the physical breach resemble recent intrusions at other facilities?
- Locate communication media going to the substation, including third-party equipment inside or outside the physical perimeter. Determine if any tampering may have occurred.
- Look for signs of a search for documents. Passwords are frequently posted on the under sides of keyboards, behind monitors, inside of drawers, or other places. An intruder looking for easy means of cyber intrusion will likely search for any information that can be helpful. In conducting this search, the intruder might have moved keyboards or other devices.
- If possible, use a wireless scanner to search for the presence of any wireless networks in the immediate area. More information about using a wireless scanner is included in the document *Backdoors and Holes in Network Perimeters* (http://www.us-cert.gov/control_systems/pdf/backdoor0503.pdf).
- If any evidence is found during visual inspection, the asset owner should contact local law enforcement to continue the investigation. Law enforcement may want to collect any retrievable fingerprints. Sections 2 and 3 provide additional guidelines for investigating cyber intrusions.

2. SYSTEMS CHECK

A systems check examines control system components through the engineering workstation or a laptop computer. It is recommended that the computer used to conduct the systems check should not have been connected to the affected cyber network or devices. An individual experienced with forensic examinations of cyber systems should work with the appropriate control system engineers or field personnel to perform the remainder of the investigation. This is to ensure integrity of the data and follow proper chain of custody rules. System operation or restoration is the primary focus, forensics becomes secondary.

Examining the control system components may include the following:

- Using the engineering workstation or laptop computer to log into each cyber device to check the log history for any recent, unauthorized configuration changes to check the date and time of files applicable to cyber devices to see if any recent changes occurred.

- Using the engineering workstation or laptop to log into each network device to check for proper functionality, network connectivity, and suspicious network connections.
- Checking each device for uptime or signs of the device being restarted.
- Looking for new user accounts, new group settings, hidden files, directories or drive partitions, changed passwords, newly installed software, tampered system files, or changes to the operating system of the device.
- Examining perimeter network and security devices such as firewalls, routers, and network intrusion detection systems for any signs of unusual network activity.
- Checking any removable media drives for media in the unlikely event that the intruder left a disk behind.
- Verifying the configuration of each device against the configuration management records and carefully noting any deviations from the documented configuration.

3. FILE SYSTEM AND BINARY EXAMINATION

A file system and binary level examination of each cyber device confirms whether files are valid or corrupted, if proper configurations are loaded onto each device, and if network services are configured correctly and operating properly. Performing a file system and binary level examination may include the following:

- Checking the time stamps of configuration files and the size of system binaries against trusted binaries. If there is suspicion that some files may be corrupt, modified, or contain malware, work with the control center and field engineers to determine if the device can be disconnected to minimize any opportunities for propagation.
- Checking the firmware of any devices with upgradeable firmware for evidence of recent changes.
- Using the engineering workstation or laptop to scan applicable cyber devices for viruses, malware, or Trojans (this check may be performed if the system has been tested and is capable of scanning without impacting critical applications or the local networked devices).
- Obtaining configuration managed files (from a trusted source), reloading configurations to each cyber device, and wiping previous configurations of each cyber device.
- Coordinating with the communications provider to perform physical and network checks of the communication systems.

If there is any evidence of cyber intrusion, it is best to perform a clean reinstallation of the operating system and all required software from a trusted source for all affected components. If possible, the original system or an image of the original, compromised system should be preserved for investigative purposes. If applicable, delete, recreate, and reformat all hard drive partitions prior to reinstalling the clean operating system and applications.

CONCLUSION

The recommended procedures for cyber security response to physical security breaches is provided for security managers to verify the occurrence and assess the impact of a physical intrusion into a site containing critical cyber assets. These recommendations should only be applied in context with the operational, safety, and maintenance environments created by the asset owner to meet business and regulatory requirements.

The physical evidence of intrusion into control systems, communications and networks, and intelligent control devices or terminals should be a serious indicator that the integrity of these devices and the systems they control is at risk. The owners and operators of critical cyber assets should review their current incident response policies and practices for physical security breaches to ensure they also address the verification of cyber system integrity. Their response plans should include steps for reporting to the appropriate Information Sharing and Analysis Center (ISAC) and/or to the United States Computer Emergency Readiness Team (US-CERT), if intrusions to cyber assets are discovered.

Although the electric utility sector was used for example purposes, all industry sectors (e.g., gas, oil, transportation, water) with remote, unmanned sites with control system cyber assets can benefit from increased awareness in response to cyber incidents concurrent with physical security breaches.

US-CERT ASSISTANCE POINTS OF CONTACTS

The Department of Homeland Security, National Cyber Security Division has assistance available from US-CERT to address information technology security and control systems security issues.

Requests for assistance from the US-CERT can be made by contacting the US-CERT at (888) 282-0870 or by sending an email to soc@us-cert.gov. Information about the US-CERT can be found on their web site (http://www.us-cert.gov).