NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Physical Security Guideline for the Electricity Sector

Assessments and Resiliency Measures for Extreme Events

June 2019

RELIABILITY | ACCOUNTABILITY

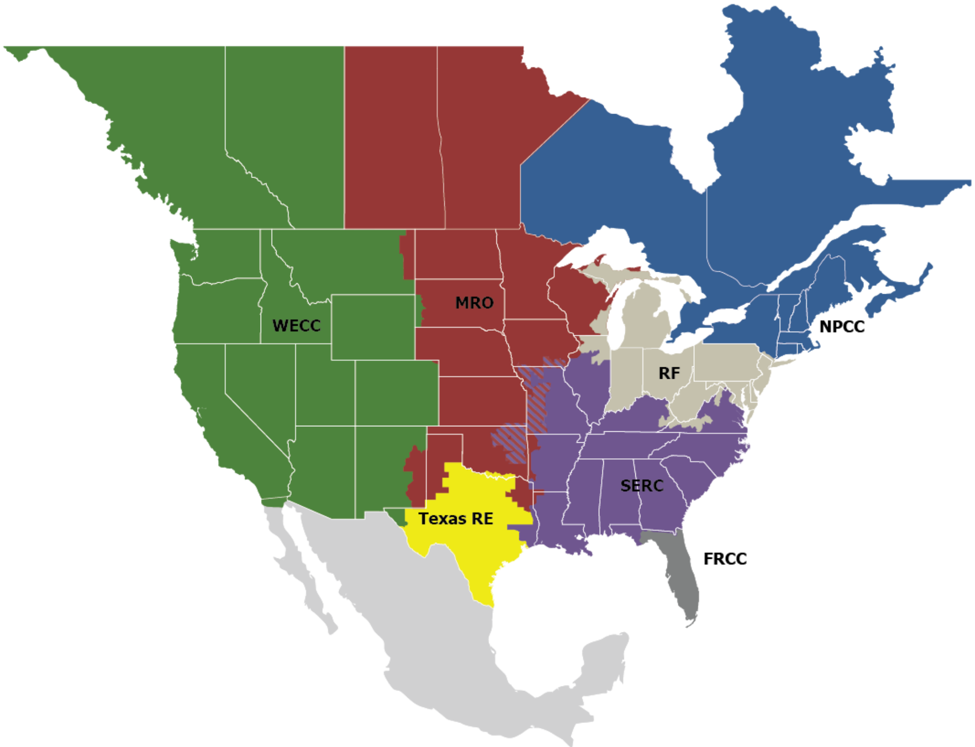
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Preamble

In November of 2016 the ERO published "ERO Reliability Risk Priorities,"[1] which was based on recommendations made by the Reliability Issues Steering Committee (RISC) to the NERC Board of Trustees. The document listed nine Risk Profiles that, at the time of publication, reflected the top priorities of the industry. Risk Profile #8, "Physical Security Vulnerabilities," addresses the possibility that intentional damage, destruction, or disruption to facilities can cause localized to extensive interconnection-wide BPS disruption potentially for extended periods.

This guideline document has been developed by the Critical Infrastructure Protection Committee (CIPC) to provide guidance to electric system entities in assessing the physical security vulnerabilities that the Risk Profile #8 describes.

The content of this guideline document is not intended to establish new requirements, modify existing requirements, nor provide interpretation of existing standards or requirements.

[1] https://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO_Reliability_Risk_Priorities_RISC_Reccommendations_Board_Approved_Nov_2016.pdf

Introduction

The nature and magnitude of extreme events pose an immediate and serious risk to an entity’s ability to effectively fulfill its responsibilities to the BPS operation, support and control. In an environment where customer dependency on reliable electric service is critical and physical attacks are expected to increase, it is increasingly important for practical and objective assessments be performed and any shortcomings addressed.

This guideline focuses on the development of physical security vulnerability assessment practices that come from effective planning and that can mitigate the impact of extreme events. While the guideline does not include details about responding to extreme events, it does provide suggestions and recommendations that can enhance an organization’s resiliency in those circumstances.

This guideline has been developed to focus on assessment of vulnerabilities that have the potential to result in events in the High Impact quadrants of the graphic below, primarily the upper left High Impact Low Frequency category.

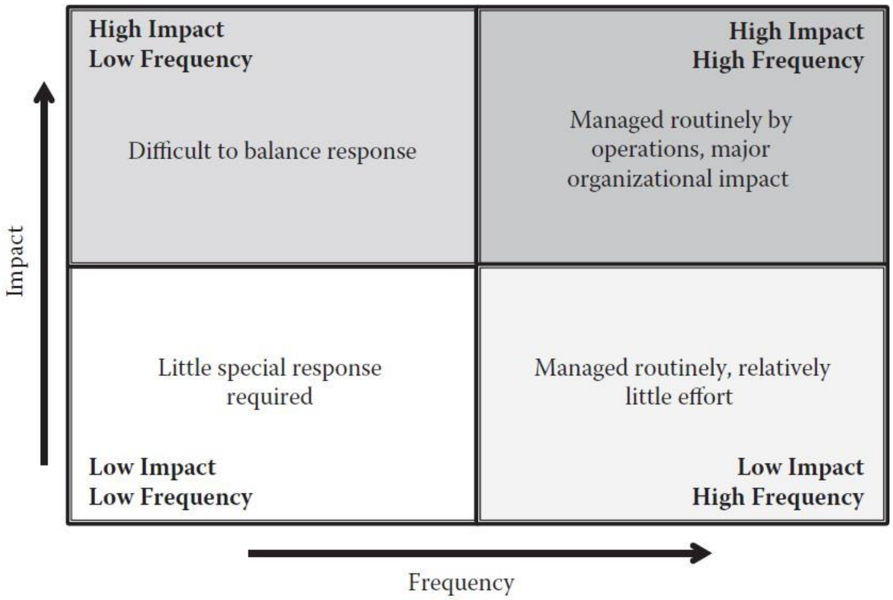

High Impact
Low Frequency
Difficult to balance response
High Impact
High Frequency
Managed routinely by operations, major organizational impact
Little special response required
Low Impact
Low Frequency
Managed routinely, relatively little effort
Low Impact
High Frequency
Impact
Frequency

Figure I.1: Impact/Frequency Matrix

The graphic below further demonstrates the need for continuous monitoring and review for events that fall within quadrants 1 and 2 which result in Very High or Extreme consequences.

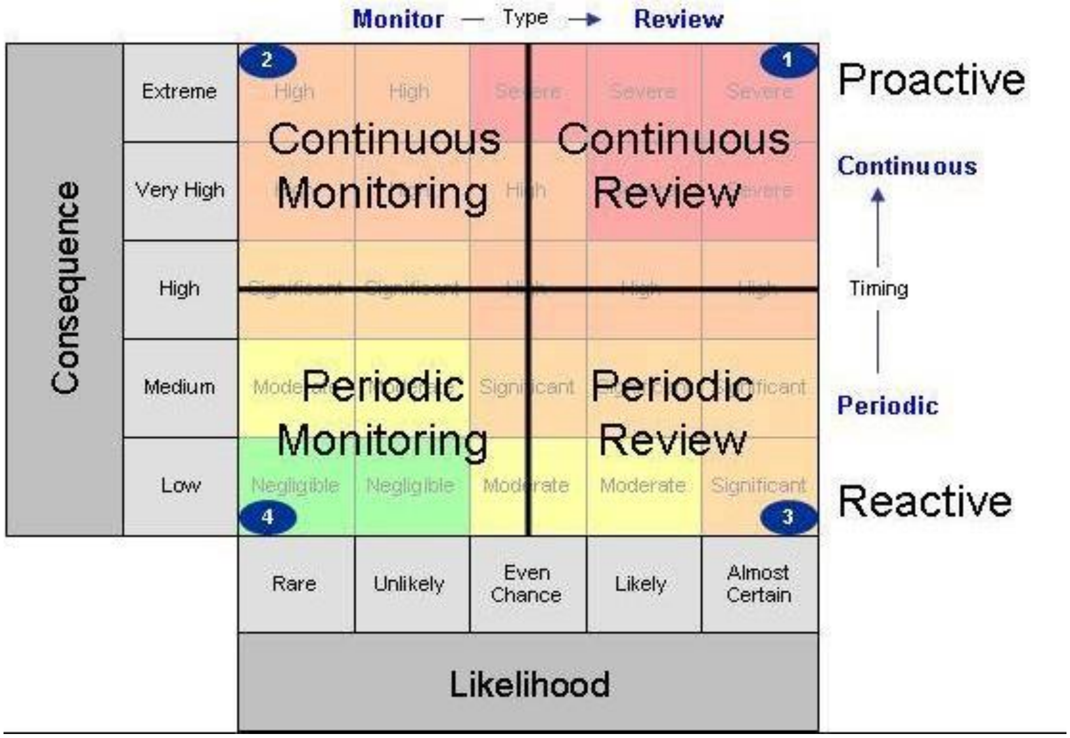


Figure I.2: Likelihood vs. Consequence Matrix

Chapter 1: Scope

The goal of this guideline is to identify and promote specific resiliency and vulnerability assessment best practices when planning for extreme events, including best physical security assessment practices, as shown in Risk Profile #8.

Identified risks as listed in Risk Profile #8 are:

1. The increasing and evolving threat around physical attacks.
2. The exposed nature of the grid, which is vulnerable and difficult to protect.
3. Long lead times associated with manufacturing and replacing some equipment, which can increase complexity of restoration after physical attacks that damage BPS equipment.
4. The level of industry knowledge or coordination in accessing the existing spare equipment inventory.
5. Physical damage to generation fuel sources, such as natural gas pipelines, which will degrade the reliable operations of the BPS.
6. Damage to long-haul telecommunications and water supplies, which will make certain critical facilities vulnerable and reduce the ability to serve load.
7. An EMP event, which could lead to widespread loss of load in certain regions.

Physical security risks and the effects of those risks are ever present and should be assessed and planned for in any vulnerability assessment. However, the planning for an event that occurs on an extraordinary scale or escalates from a relatively minor event to an extreme event requires a planning model that is robust and capable of adapting to the current situation and conditions as the event matures.

Various factors contribute to the magnitude and scope of an event and the criteria for classifying it as an extreme event. When performing assessments and planning for extreme events, it is important to consider that events may not be and may not appear to be extreme events when first recognized, but conditions may result in it being escalated to ‘extreme’ status.

Events may quickly escalate into extreme status depending on several factors:

1. The level of impact. If an event is confined to a local facility the impact to the BPS is likely minor and the response localized, however if the event is regional or national, the impact will be more significant.
2. The entity’s level of preparedness. An entity that is not prepared may struggle in its response as compared to an entity with a mature plan and effective mitigation measures available.
3. The level of resources necessary to effectively respond to an event can also affect the success of the response.
4. The possibility of a cascading effect on BPS assets or other critical infrastructure sectors can result in the escalating severity of what was initially perceived to be an ordinary event.

Chapter 2: Planning for Extreme Events

This guideline presupposes that a company's emergency response plans and security measures capture most of the elements required for the tactical response to extreme events. The purpose of this section is to discuss the strategic elements that an organization can consider in planning its response to extreme events.

When developing the plan, begin by considering the organization's priorities. Knowing the priorities will help determine the resilience and recovery options that should be considered. The following are some areas to consider that may help guide discussions:

- Virtually every organization counts the safety of employees, contractors, visitors, and members of the public as a priority, and the electricity sector is no different. Everything is replaceable except human life. Response to an extreme event should reflect, above all, care for people.
- Protection of the environment - Damaging the environment affects others and can have consequences that can threaten an organization's ability to operate, so environmental issues may factor in all planning.
- Physical asset protection - Physical and cyber assets are necessary for generation, transmission, and distribution of electricity. Damage to assets can keep a company out of the marketplace for an extended period of time, so protection of physical assets should be addressed in a risk based manner.
- Restoration of service - Safe and secure operations depend on factors such as people and properly functioning equipment.

The elements of response at this level are as follows:

- **Crisis Management Team** - For assessing damage, marshalling information and resources, ensuring the safety and survival of employees, and protecting the public. This team will manage the crisis using the priorities stated earlier as a guide. The Director of the Crisis Management Team should be a Senior Executive (or equivalent).
- **External Liaison and Notification** – Is this an event which will overwhelm an organization's capability to adequately respond, requiring external resources to be brought in? Are there regulatory reporting requirements that need to be addressed? Do neighboring facilities need to be informed?
- **Communications Plan** - Both external and internal (including the Board of Directors), and including social media policies, employee notification, and employee contact information.
- **Restoration Team -** A subset of the Crisis Management Team, this group works to prepare the organization for a return to normal operations. This team may include operations, supply chain, finance, HR, and Security.

Security Planning

Security planning for extreme events should be considered part of **the Crisis Management Team** suite of plans, as it can be executed under its supervision.

The table below provides an example of some planning considerations for a bomb attack

Table 2.1: Planning Considerations for a Bomb Attack

Event	Priority	Function	Comments
Bomb attack	Safety	Emergency response plans for all aspects related to bombs: bomb threats reporting, premises searches, suspicious package	Most of the activities in this area are found in the domain of emergency response planning and the corporate safety management program.

Table 2.1: Planning Considerations for a Bomb Attack

Event	Priority	Function	Comments
		protocol, response to explosions (evacuation, etc.) Training and equipping employee First Aid teams	
	Prioritizing Communications	Strict social media policy (no unauthorized tweeting or Facebook posts during emergency events) Corporate communications plan to promote employee and public notification in the event of an emergency	A response to an extreme event may be disrupted by family or media pressure. Good communications planning can help to prevent this, but ensuring that employees know why it is important not to put photographs on social media, and the consequences if they do, will help the communications effort.
	Physical Asset Protection	Access control to prevent unauthorized persons from entering facility	Planning for a bomb attack starts during the design phase of physical security measures. If the original design did not include measures needed during a bomb threat, then temporary measures can be introduced until the permanent measures are installed. For example, a truck or Jersey barriers can be used to block a road to prevent vehicle access until bollards are installed.
	Restoration of Service	Business Continuity Plans	Business Continuity Plans which allow for the loss of production, administrative office space, information systems, or personnel are needed here.

Chapter 3: Vulnerability Assessments

A vulnerability assessment is an examination of an entity's asset(s) to identify conditions that might be exploited by an attacker to cause harm to the asset or the personnel associated with the asset.

When creating or updating a vulnerability assessment it is useful to start with a list of the assets to be protected and the identified threats. In an extreme event, the list of assets should be reviewed to determine the order of priority in which the vulnerability assessment is conducted. The identified threats may have changed significantly during an extreme event and should be reviewed.

The vulnerability assessment may bring to light areas in which the extreme event has caused either a degradation or loss of functionality in a security measure. The incapacity to perform as designed could be exploited by a threat actor or in some cases may be the intended consequence of the threat actor as a step towards additional second or third order effects. The assessment may lead to the identification of additional security measures.

Physical security vulnerability assessments include a comprehensive review of the physical security posture with the purpose of identifying as many vulnerabilities as possible. Vulnerabilities are weaknesses that can be exploited by a threat source. It would entail a comprehensive review for the purposes of identifying, quantifying, and prioritizing the vulnerabilities at an asset or with related personnel to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

A vulnerability assessment allows an entity to examine its own physical security faults as an attacker would see them. Such an assessment is sometimes difficult to do effectively due to cognitive biases. Review by an outsider to validate an existing vulnerability assessment or conduct a new vulnerability assessment will help to eliminate the biases of an insider that might affect the assessment results.

After an extreme event has occurred, the vulnerability assessment should be reviewed, or if it doesn't exist, created, to address circumstances encountered during the event.

While in a defensive role, think like those in an offensive role. Questions to ask may include when, where, and how would an attacker, internal or external, attack this target or the people employed here. Essentially, the task is to perform a target assessment. A vulnerability assessment looks for and finds the weaknesses in processes, locations, structures, materials, and devices that security and facility managers may normally rely on to provide a secure environment.

For each impacted asset, the vulnerability assessment should give consideration to the following factors:

Table 3.1: Vulnerability Assessment Factors

Factor	Description
General Asset (structure) design	Features of the asset design that create weakness that can be exploited by an adversary, such as open areas allowing observation from a distance, large windows that allow operations to be observed from the outside, etc.
Proximity to uncontrolled areas	Areas that are not controlled by the company especially areas allowing public access for travel or occupation
Access Control Points	Entry points into the asset by vehicles or people
Barriers	Obstacles such as fences, walls, gates, and environmental features.

Table 3.1: Vulnerability Assessment Factors

Factor	Description
Access by unauthorized personnel	Access by individuals who have not undergone company credentialing process including escorted access.
Access by required services	Access by people such as deliveries, utilities or emergency services.
Area denied to access	Identified areas where vehicles or people are not allowed.
Areas minimized to access	Identified areas where access is restricted, such as to company vehicles or employees only.

Each factor should be scrutinized to determine any security vulnerability that could be exploited by an attacker. One of the fundamental questions for each factor is whether the extreme event has altered or could alter the security protections in place for that factor.

Example questions for each factor include:

Table 3.2: Security Vulnerability Factors

Factor	Sample Questions
General Asset (structure) design	How could surveillance be conducted? What are the materials used to construct the asset? How susceptible is the asset to an explosion? What are the blast zones based off a Design Basis Threat? How susceptible is the asset to gunfire? What internal and external lighting options are available? What materials were used for walls, floors, ceilings and roofs? What are the asset external penetrations?
Proximity to uncontrolled areas	How close can the public get to the asset? What part of the asset can be seen from public spaces? What are the ingress and egress points to observation locations? Is there a public parking lot or parking garage close to the site? Is there a public use trail or park close to the site?
Access Control Points	How many and where are the vehicle entry points? How many and where are the personnel access points? What mechanism prevents or slows access at the entry points? What mechanism detects or logs access at the entry points? Are there trenches, ducts, sewers, storm drains allowing access? Are there railroad tracks or pipelines entering the perimeter? Are there straight-line vehicle approaches to critical areas?
Barriers	What creates the physical security perimeter for the asset? Is there a layered approach to the barriers? What are the barriers constructed from? Does the terrain help or hinder an attacker? What vegetation is present? Are barriers fixed or moveable?
Access by un-cleared personnel	How do people get access to the asset? Who approves access? Who escorts and how many can be escorted at one time? Is there a visitor access program? Is there an established stand-off zone for vehicles?
Access by required services	How do outside service people access the site?

Table 3.2: Security Vulnerability Factors

Factor	Sample Questions
	Are vehicles searched upon entry or exit? How to verify the service person is legitimate? Are escorts needed for some services versus others? Are deliveries confined to a certain area? Who approves service people to enter the asset?
Area denied to access	Are there areas where foot traffic is not allowed? Are there areas where vehicle traffic is not allowed? What are the protection methods for the areas? Is there an established exclusive stand-off zone?
Areas minimized to access	Are there areas where only certain types of foot traffic are not allowed? Are there areas that only certain vehicle traffic is not allowed? What are the protection methods for the areas?

Chapter 4: Physical Security Assessments

A periodic assessment is appropriate for determining whether existing physical security measures are adequate and effective for addressing events that are extreme or that may escalate to extreme status[2].

Physical Security Assessment

A thorough on-site security survey can provide information that an organization can use to: 1) Determine and document the current security posture, and how that posture might be affected if an extreme event is imminent; 2) Identify deficiencies and excesses in existing security measures; and 3) Evaluate the current posture to determine whether it provides the appropriate level of security or protection and identify possible improvements.

Physical security assessments can be used to identify actual or potential threats that extreme events could pose and can provide valuable information to help an organization plan and prepare its response to each level**.** Physical security measures may be integrated with existing business continuity plans, and the security baseline can be adjusted appropriate to the level of the corresponding threat**.** The physical security measures baseline should be adjusted whether the threat is anticipated or real. Consider adopting a spare equipment/mobile equipment strategy to improve resiliency.

Physical Security Baseline

Before preparing for threats and hazards, the following physical security practices should be applied to the current state of physical security. Critical assets should be identified based on industry regulations (e.g., NERC Critical Infrastructure Protection Reliability Standards) and enterprise business continuity requirements. Classification levels should be given to assets based on their level of criticality (e.g., level 1 for the lowest level of criticality and level 4 for highest level).

Minimum physical security measures should be implemented based on the level of criticality (e.g., Level 1 can be mechanical access control and Level 4 can be two-factor authentication (2FA) electronic access control with intrusion detection (IDS) perimeter system and on-site response force). Also, there should be a description of how escalation of response measures should be considered based on the threat of extreme events or history of incidents.

Assessments which focus on physical security measures such as evaluation of perimeter integrity and use of physical security measures by employees should be performed at a frequency determined by the level of criticality of the asset.(e.g., level 1 reviewed once a year and level 4 once a month) Reporting of any security events and physical security vulnerabilities by employees and contractors to the security department should be mandatory (e.g., breach in fencing, door that doesn't lock properly, loss of access card, etc.).

Regularly scheduled physical security assessments on all key assets that require protection (generating station, substation, control center, data centers, transmission lines, etc.) are considered a best practice. Updates on the assessments should be made whenever changes occur in operations or configuration of an asset that could impact the physical security measure's effectiveness.

Physical Security Assessment for Unplanned Extreme Events

Identify the contingencies that could affect the physical security measures baseline, such as lockdown policies and physical security measures for active shooter situations. Develop contingency measures and be prepared to deploy them when extreme events occur; for example, rehearse lockdown procedures with security personnel once a year at critical locations. Identify any gaps (situations for which no contingency measures have been identified) and assess

[2] Based on extracts of *Physical Security Principles, ASIS, 2015*

the risk. If the risk is not acceptable, close the gap by adding the appropriate measures.

Also consider improving system redundancy; for example, if there are no physical security measures to permit lockdown procedures for employees, evaluate the risk of active shooter situations. Use the results of that review to decide whether to accept the risk or implement measures to perform lockdowns.

Chapter 5: Drill and Exercises

The nature of extreme events is that they often unforeseen and thus difficult to prepare for. Emergency managers design programs to maintain readiness for all hazards. Common hazards are described in the National Incident Management System (NIMS) and by the Incident Command System (ICS), a standardized, on-scene, all-hazards incident all hazards approach.[3] Additionally, those who assume the role of Emergency Manager are responsible for preparing and evaluating their entity's ability to respond and recover from extreme events.

Preparation and evaluation are critical for maintaining operational resilience. Facing disasters with unevaluated emergency plans often results in poor procedural execution, leading to confusion in response and recovery. 29 CFR 1910.38OSHA is a standard that describes what an emergency action plan (EAP) should contain and the importance of conducting drills and exercises to evaluate an entity's response to site level emergencies. Scenarios that are based on situations that are most likely to occur within the workplace, such as active shooter, fire drill or other emergencies, are recommended. Additional consideration can be made for planning drills and exercises that evaluate preparation for extreme events.

The Framework

An extreme event that does occur may immediately deplete resources that are directed to the initial response. Extreme events are unpredictable and are likely to have an expansive footprint and/or intensifying levels of complexity. Unlike low-level site events involving site management and an initial response from local first responders; extreme events involve a large group of first responders in addition to feedback from technical experts from private organizations and government agencies. An entity's emergency management program should have a framework or system in place to facilitate the rapid increase of personnel.

Exercises to evaluate the performance of individual business units presents opportunities to test the current framework. Results of these exercises also identify challenges associated with implementation and logistics necessary to accommodate the influx of additional responding agencies. Throughout history, the challenges identified in responding to large scale events like Hurricane Katrina have involved problems with command and control, resource distribution and prioritization of response. Due to the nature of extreme events, the Incident Command System provides a framework allowing agencies to streamline capabilities to adjoin with multiple agencies and jurisdictions during an event.

Exercising the Framework

The objective of drills and exercises is to evaluate the capabilities of a program. Drills are defined as coordinated supervised activities, usually employed to test a single operation or function within an entity. Drills are designed to review the performance of smaller sections of a larger group. Most drills are performed shortly after the initial instruction of a task or procedure. Drills are presented as opportunities for participants to ask questions and receive correctional guidance during the performance of actions.

There are three common forms of exercises. The most common method of exercising for extreme events may be through tabletop exercises. These can either be formal or informal evaluation or discussion-based exercises performed by key personnel. Tabletops are beneficial because they can involve leadership, players and observers from an unlimited number of entities who can be presented with comprehensive understanding of the disaster and affected area. Additionally, tabletops show value because they provide opportunity for representatives and technical specialists to collaborate and refine operational plans and policies. Moreover, tabletop exercises offer opportunities for people to identify the necessary points of contact for different agencies and business units.

[3] (National Incident Management System, 2019)

Another type of operational based exercise is a functional exercise (FE), which examines and/or validates the coordination, command and control between various multi-agency coordination centers. FEs utilize minimal involvement from personnel and resources. During these exercises, department resources and involvement by other agencies can be simulated.

A third type of operational based practice is a full-scale exercise (FSE), which is designed to reflect coordination between multi-agency, multi-jurisdictional, and/or multi-disciplinary resources. An FSE is intended to facilitate a functional organizational response, with personnel and resources implemented in real time. Entities may choose to conduct FSE's only every 2-3 years to prevent strain on resources.

Exercising for extreme events is likely to incorporate a multi-agency response. Success is achieved when participants effectively identify and resolve issues in the overall response process. It is best for each entity to understand how their procedures and processes evolve when additional resources have become available, and when changes in command and control staff are expected. For example, a comprehensive training program in exercise design can be found through Homeland Security Exercise and Evaluation Program (HSEEP)[4].

The Extreme Event Scenario

A well-developed scenario for extreme events should challenge the emergency management capability of an entire entity. Historically, extreme events have presented employees, management, and responders with an extremely demanding operational tempo during response and recovery phases. Replicating this tempo in an exercise can be difficult; exercise officials (i.e. planners and controllers) must ensure the exercise injects occur quickly. Exercises based on acts of terrorism, electro-magnetic pulse, chemical, biological, radiological and nuclear event or severe weather are all viable options capable of being referenced through scientific data and historical facts. Entities can reference characteristics of such events to further scenarios and determine program effectiveness.

Evaluation

As described, exercises are used to evaluate a process in real time, using criteria derived from the exercise objectives. Evaluations from FE's and FSE's rely on player integrity and knowledge that actions are to be carried out and reviewed for fluidity and effectiveness. As discussed previously, an extreme event may mean an entity must collaborate with others for a coordinated response. Thus, entities are encouraged to establish memoranda of agreement (MOA) and/or memoranda of understanding (MOU) with neighboring organizations to identify resources capable of being committed to an extreme event. The language in the MOU/MOA should not simply define the resource commitment, organizational alignment, and jurisdictional authority, but also highlight standards for performance by each organization.

Engagement

The most important element of an exercise is solicitation. Public and private entities from adjacent sectors may find the level of complexity of the electric grid to be intimidating. Utilities can address this issue by reaching out to other sectors and encourage them to join and understand the impact of an extreme event on the electric grid. A great place to start is with engaging local and state or provincial emergency management officials. Educating local and state or provincial emergency management officials and encouraging their participation will benefit their agencies by further promoting the stringent testing of their own capabilities.

[4] (Homeland Security Exercise and Evaluation Program, 2018)

Chapter 6: Resiliency

This section discusses resiliency as it applies to effectively navigating through extreme events. In layman’s terms, resiliency describes toughness, or the ability to quickly rebound from situational setbacks. The reliability of the electric grid is contingent upon an entity’s resilience. Resilient entities are interdependent; they form a network in which each entity supports the grid; while mutually reliant, they each support and maintain their own assets. Like other networks, the grid is only as strong as its weakest point; a single entity that does not cultivate its own resilience in preparation for extreme events may potentially compromise the security of entire network.

The objective of resiliency is to minimize the time an entity is non-operational and to increase the pace at which the entity can return to full capacity and restore the grid. Three dimensions of resiliency will be discussed here. The first, structure resilience, refers to facilities or housing that protect personnel and systems from the elements. The second dimension is the resiliency of people or employees who are prepared and capable of maintaining composure and rational thought through an extreme event while performing their duties. The third dimension, systems resilience, is a set of principles or procedures describing what is to be done. In this context, systems also refer to mechanical or digital devices intended to enhance operability, such as cameras or industrial control devices.

Structural resiliency is to strengthen or reinforce the protective integrity of an enclosure to enhance its capability to absorb damage caused by extreme events. Resilience is achieved by adapting enhancements through materials such as steel plating, or by engineering specifications designed to withstand force. Additionally, resiliency can be enhanced by the implementation of physical security features to the external surface of the structure. Designs such as window films that enhance the integrity of the glass, or barriers that can withstand the effects of blasting, cutting, or ramming on fences, walls or blocks, all contribute to the resiliency of a structure. Alternatively, resilience can also be achieved through the ability to rapidly repair assets and restore service. For example, it may make more sense to develop rapid repair capabilities for the restoration of transmission services rather than undertake expensive hardening of transmission towers.

The second dimension is ensuring resiliency through the workforce. This is the most complex, as it requires interaction amongst the multiple personality types that populate the entity. The pathway to personal resiliency is achieved and maintained by creating a culture geared towards personal development, adaptability, communication and teamwork. People are inherently resilient; good management fosters their resiliency by providing them with training and exercises that cultivate critical thinking. Conditioning employees to withstand stress in their individual roles strengthens the integrity of the team.

The third dimension is the resiliency of systems. This applies to both analog and digital systems that enhance an entity’s operability, and to the reinforcement of internal controls to prevent mis-operation and errors. Like facilities and employees, systems require rigorous testing, and continuous improvement to ensure sustainable operations through extreme events. Informed entities recognize that attacks on the grid are intended to disable and destroy. Thus, resilient entities can develop and train on robust processes to ensure stringent adherence to procedures that minimize failures and maximize that capacity to rapidly replace or recover those systems lost in the shortest amount of time.

An overarching principle for the developing of resiliency in structures, organizations, and systems is the application of redundancy. Redundancy is the basic principle applied to create continuity within the system to ensure that no single points of failure exist. Principles of redundancy applied to communication systems, subject matter experts, or life support systems such as backup generators are beneficial during extreme events. Redundant systems present options to the strategic decision making of Incident Commanders, sustains quality of life for response and recovery teams, and ensures continuity of operations for management and stakeholders.

In conclusion, achieving resiliency requires effective interrelationship between structures, people and systems as described above. Entities should consider continually and comprehensively developing and maintaining the resiliency of their personnel, systems and facilities. While there is no perfect strategy by which every entity can defend its assets, there are always ways to adapt best practices to strengthen entity resilience. Applying the strategies of redundancy, continuous improvement, and adaptation to daily problems and emerging challenges are the ingredients for achieving resilience in the face of extreme events.

Chapter 7: Information Sharing During Extreme Events

Protecting something as intricate as the electrical grid requires a network of communication and information sharing. Retired General Stanley A. McChrystal once stated, “It takes a network to defeat a network” [5]in contrast, it takes a network to defend a network as well. Extreme events present exceptional challenges to the capabilities of an entity’s decision-making cycle. To counteract extreme events, an entity depends upon a **fundamental knowledge** to understand data as it applies to extreme events. The **speed at which information must be transmitted** is a pivotal factor; facilitating, enabling or hindering leadership’s ability to think and react critically and effectively. The **collaborative efforts of numerous entities** can enhance the responsiveness of each entity to extreme events.

The Fundamentals

Entities should understand the foundation of an information sharing program is the accumulation of data. During extreme events, the application of data may allow entities to detect and resolve problems before they evolve into crisis, to evaluate the effectiveness of response, and to identify relationships between variables. Most importantly, the value of data during extreme events is evident: 1. Data allows management to think critically; 2. Data provides responding personnel and organizations with relevant information and tools; 3. Data helps enhance understanding of the operational environment; and 4. Data facilitates informed decisions that lead to effective response and recovery operations.

While data application plays a large role in emergency preparedness and management operations, it has its limits. Extreme events are statistical anomalies that cannot be used to obtain data that fully predicts extreme events. For example, man-made disasters (e.g. Deepwater Horizon, Three Mile Island) occur unexpectedly, typically due to mistakes or unforeseen failures in systems with little warning. The Root Cause Analysis on these events highlighted findings that indicate these disasters could have been avoided had system and human performance issues been detected early.

Criminal induced disasters such as terrorism are typically carried out strategically and often under a high level of secrecy. Such events can be forecast with low certainty based on the data from historical trends and behavioral indicators; however, this data cannot definitively or precisely predict (e.g., dates, times, locations, etc.) such extreme events.

The sheer volume of data can be overwhelming and hinder useful application. Data that is well organized and analyzed can be vital for identifying effective prevention and response measures to extreme events. This information is essential to incident commanders, allowing them to determine relevance and helps with situation awareness. Incident response teams rely on the work of dedicated analysis to utilize collected information in a coherent and effective manner, while facilitating the flow of information internally. The added value of continually updated information is that it reduces risk to responders during extreme events.

The Need for Speed

Effectiveness of the response during extreme events is heavily dependent on the speed at which information is delivered. The unprecedented pace at which an extreme event may unfold might exceed the capabilities of the entity’s response mechanisms. Thus, the timing at which informational products are released may only provide a snapshot of a given set of circumstances. Analysts who are experts in the subject matter may be able to formulate possible outcomes based on potential variables. At a bare minimum, information should be shared with incident commanders and others, allowing them to mitigate risk in their overall response strategy and build continuity among responders.

[5] (McChrystal, 2011)

As extreme events become increasingly complex, the potential for secondary or simultaneous attacks occurring against the Electrical Grid reinforces the need for expedited information exchange between entities. In a 2016 document drafted by the Physical Security Advisory Group "Electricity Sector and the Design Basis Threat," an attack on the grid will be the actions of dedicated, skilled, and coordinated actors, using multiple attack vectors such as physical, cyber and possibly unmanned aerial vehicles. Arguably, there is no absolute way to prevent future attacks, since a trained adversary will likely use speed, surprise and violence of action to their advantage. The best strategy is to strengthen the interdependence between entities as described and reinforce the speed and accuracy of information exchanged.

The nature of extreme events is to be fast-paced, possibly widespread, and to present dynamic risk factors. Thus, it is desirable when the flow of information is streamlined to approximate the speed at which the extreme event unfolds. Best practices include the implementation of internal controls during extreme events to minimize or prioritize their information sources. This helps ensure that incident commanders only receive vetted and pertinent information. This necessitates that entities design incident response programs that incorporate information channels to control flow of information during extreme events. Recent revisions to the FEMA Incident Command System now include an Intelligence & Investigation Section, reporting directly to the Incident Commander.[6]

The Network

Sources of data applicable to extreme events are likely to originate from inter-entity condition reporting, cross-industry information sharing networks, Human Intelligence (HUMINT) and Open Source intelligence (OSINT). More specifically, HUMINT relies on the vigilance of employees, community members and law enforcement officers to detect and report activity, making it relevant for emergencies. The effectiveness of HUMINT may be limited by human performance; the chaos of disasters may result in subtle details going unnoticed, thus stifling the ability to obtain clear data. OSINT, such as databases, intelligence products from credible sources, and social media, adds to the collection of raw data and perhaps validates HUMINT contributions to the Common Operating Picture (COP). [7]Additionally, social media serves best in extreme events when it effectively details the parameters of the event, thus filling a need for information-sharing network enhancements, and rapid information exchange.

The information sharing network should begin within an entity. Employees should be encouraged to identify problems at any moment. During extreme events, employees may become key role players, supporting response and recovery operations. Fostering employee vigilance and promoting prompt reporting behaviors will strengthen response by mitigating risk. Adopting the DHS "See Something Say Something" [8]practice is an effective starting point, particularly when entities tailor the program to their specific capabilities.

The expansion of the information sharing network should begin with business units. The strength of the network is reliant on each business units' ability to collaborate with external peer business units from local entities and intelligence organizations. Although not a requirement, entities should make an effort to become a part of such networks. Participating in information exchange helps to paint a larger picture of the threat landscape. An advantage of this network is preparation for extreme events, as neighboring entities can provide peer evaluations and contribute to effective assessment of risk and vulnerability. When extreme events are imminent, neighboring entities may offer mutual assistance as well as pass along useful information that contributes to the COP.

Entities involved in extreme physical security events are likely to engage local, state and federal law enforcement agencies, including local officials from the FBI and the Royal Canadian Mounted Police. These agencies respond and contribute to the flow of information via investigations and criminal intelligence. Currently, local and state enforcement agencies are expanding their information distribution into critical infrastructure and key resources. They provide utilities additional information to further identify and mitigate threats.

The Electricity Information Sharing and Analysis Center (E-ISAC) is an information sharing entity dedicated to the electric utility industry. It ensures the delivery of timely and accurate physical and cyber security threat intelligence to owners and operators. The benefit of the E-ISAC is to amass threat information from various sources and to distribute it throughout the industry. Applied to extreme events, the E-ISAC adds value by obtaining details of events and continually updating owners and operators, thus enhancing vigilance throughout the industry in preparation for subsequent hostile actions.

Historically, the need to gather and share information has been viewed as the primary role of our nation's security apparatus. The owners and operators of the Bulk Electric System ensure the survivability of the nation by maintaining the delivery of reliable electricity. Thus, each entity plays a part in upholding national security. Extreme events induced by acts of terrorism, accidents, or natural events can only be successfully addressed if industry collaborates to create a network so great and effective that adversarial efforts will inevitably fail.

[6] (National Incident Management System Intelligence/Investigations Function Guidance and Field Operations Guide, 2013)

[7] Common Operating Picture (COP) - Single identical display of relevant operational information (i.e. locations of responders, status of resources, scene details) shared by more than one command element.

[8] (If you see something, say something, 2019)

Chapter 8: Definitions

Extreme Events – A high impact event that has the potential to severely damage or impair an organization's ability to operate.

Physical Security Assessment – The evaluation of a facility to determine the current physical security posture, identify deficiencies, and recommend improvements in the overall situation.

Resilience – The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Examples of resilience measures:

- Developing a business continuity plan
- Having a generator for back-up power
- Using building materials that are more durable

Vulnerability Assessment – A vulnerability assessment is an examination of an entity's asset(s) to identify conditions that might be exploited by an attacker to cause harm to the asset or the personnel associated with the asset.