NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Attack Task Force

Final Report

Board of Trustees Accepted: May 9, 2012

RELIABILITY | ACCOUNTABILITY




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

NERC's Mission

The North American Electric Reliability Corporation (NERC) is an international regulatory authority established to enhance the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; assesses adequacy annually via a ten-year forecast and winter and summer forecasts; monitors the BPS; and educates, trains, and certifies industry personnel. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.[1]

NERC assesses and reports on the reliability and adequacy of the North American BPS, which is divided into eight Regional areas, as shown on the map and table below. The users, owners, and operators of the BPS within these areas account for virtually all the electricity supplied in the U.S., Canada, and a portion of Baja California Norte, México.

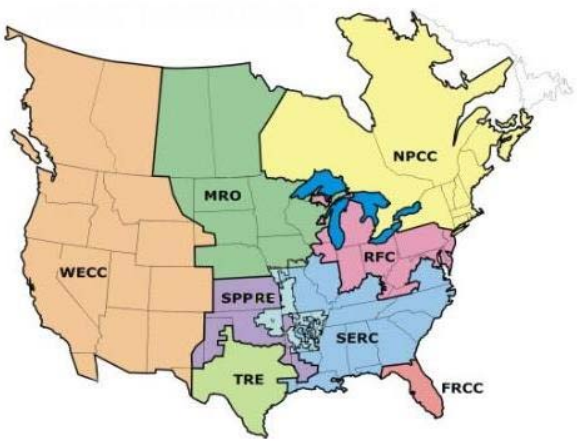


Table A: NERC Regional Entities	
FRCC Florida Reliability Coordinating Council	**SERC** SERC Reliability Corporation
MRO Midwest Reliability Organization	**SPP** Southwest Power Pool, Incorporated
NPCC Northeast Power Coordinating Council	**TRE** Texas Reliability Entity
RFC Reliability*First* Corporation	**WECC** Western Electricity Coordinating Council

Note: *The highlighted area between SPP and SERC denotes overlapping regional area boundaries: For example, some load serving entities participate in one region and their associated transmission owner/operators in another.*

[1] As of June 18, 2007, the U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce Reliability Standards with all U.S. users, owners, and operators of the bulk power system, and made compliance with those standards mandatory and enforceable. In Canada, NERC presently has memorandums of understanding in place with provincial authorities in Ontario, New Brunswick, Nova Scotia, Québec, and Saskatchewan, and with the Canadian National Energy Board. NERC standards are mandatory and enforceable in Ontario and New Brunswick as a matter of provincial law. NERC has an agreement with Manitoba Hydro making reliability standards mandatory for that entity, and Manitoba has recently adopted legislation setting out a framework for standards to become mandatory for users, owners, and operators in the province. In addition, NERC has been designated as the "electric reliability organization" under Alberta's Transportation Regulation, and certain reliability standards have been approved in that jurisdiction; others are pending. NERC and NPCC have been recognized as standards-setting bodies by the Régie de l'énergie of Québec, and Québec has the framework in place for reliability standards to become mandatory. NERC's reliability standards are also mandatory in Nova Scotia and British Columbia. NERC is working with the other governmental authorities in Canada to achieve equivalent recognition.

Table of Contents

Table of Contents iii

Executive Summary 1

Defining a Coordinated Cyber Attack 2

Enhancing Resilience 2

Key Recommendations 4

Introduction 1

Approach 1

Adversaries, Motivations, and Capabilities 3

Insiders 9

What a Coordinated Attack Looks Like 10

Prerequisites of an Attack 11

Coordinated Cyber Attack Scenario and Assumptions: 12

Detection Capabilities 14

Global Monitoring of Internet Activity 15

Federal Initiatives 15

Peer Groups 15

Alerts 16

Precursors and Local Indicators 16

Deterrence / Defensive Capabilities 18

Education / Training 20

Incident Response Plans 20

Information Sharing 23

Post-event analysis (Lessons Learned) 25
Procurement Language 26
Independent Testing of Systems and Equipment 26
Responses to Attack 27
Background 27
Isolation and Survivability 28
Restoration 29
Forensics 29
Recommendations 33
Outreach 38
References 40
Appendix A: Introduction to Attack Trees 44
Appendix B: Resources 46
Appendix C: Cyber Event Scenarios for System Operators 48
Overview 48
Social Engineering – false request or information to operator 49
Description 49
Implementation 49
Recognition 49
Response 49
Denial of Service – EMS network 50
Description 50
Implementation 50
Recognition 50
Response 50

Denial of Service – EMS applications halted 51
Description 51
Implementation 51
Recognition 51
Response 51
Spurious Device Operations 52
Description 52
Implementation 52
Recognition 52
Response 52
Realistic Data Injection 53
Description 53
Implementation 53
Recognition 53
Response 53
Appendix D: Acronyms 54
Appendix E: Potential Responses to an Attack 57
Appendix F: Precursors and Local Indicators of an Unusual Event 61
Appendix G: Isolation and Survivability Tactics 63
Appendix H: Defensive Capabilities 65
Appendix I: CRPA Observations and Recommendations 67
Appendix J: Case Studies 71
Appendix K: Task Force Goals and Objectives 75

Executive Summary

The North American bulk power system (BPS) is one of the most critical of infrastructures and is vital to society in many ways. The electric power industry has well-established planning and operating procedures in place to address the "normal" emergency events (e.g., hurricanes, tornadoes, and ice storms) that occur from time to time and disrupt electricity reliability[2]. However, the electricity industry has much less experience with planning for and responding to high-impact events that have a low probability of occurring or have not yet occurred.

To help the electricity industry better understand these low probability risks, in June 2010, NERC and the U.S. Department of Energy issued a report titled, "*High-Impact, Low-Frequency Event Risk to the North American BPS*"[3]. Subsequently, the NERC board approved a *Coordinated Action Plan*[4] under the leadership of the NERC Technical Committees to establish four Task Forces needed to address this work. This report provides the conclusions of one of them – the Cyber Attack Task Force (CATF).

This effort has challenged the CATF in a number of ways.

- The industry already recognizes cybersecurity risks, in part by addressing the requirements of the NERC Critical Infrastructure Protection standards CIP-002 – CIP009. As a result, some entities may feel they are already prepared.
- While entities are challenged on a daily basis by new cybersecurity vulnerabilities and attempted intrusions, a successful coordinated cyber attack affecting the North American bulk power system has not yet occurred. Therefore, it is difficult to confidently determine the potential impact on the reliability of the bulk power system and what additional actions may need to be taken.
- Through the course of its work, the CATF shared sensitive information related to threats, vulnerabilities, and impacts. While this information was essential to develop the recommendations found in this report, the CATF could not include these details in this public report.

The CATF has recognized these challenges and through this report offers electricity industry owners and operators (entities) a number of suggestions and recommendations. The report highlights 8 key recommendations that will help entities prevent, deter, detect, and respond to a coordinated cyber attack and further enhance the resilience of the bulk power system.

[2] Ref. NERC Adequate Level of Reliability http://www.nerc.com/docs/standards/Adequate_Level_of_Reliability_Defintion_05052008.pdf
[3] Ref. High Impact Low Frequency report http://www.nerc.com/files/HILF.pdf
[4] Ref. Coordinated Action Plan http://www.nerc.com/docs/ciscap/Critical_Infrastructure_Strategic_Initiatives_Coordinated_Action_Plan_BOT_Apprd_11-2010.pdf

Defining a Coordinated Cyber Attack

The CATF adopted an approach that assumed a coordinated cyber attack has occurred. It did not attempt to determine the likelihood of such an attack either today or at some time in the future. The CATF also did not attempt to determine which functional entities[5] might be more susceptible or vulnerable to attack. The CATF determined that it was more important to assume that an attack has occurred, and consider what actions need to be taken to prevent, deter, detect, and respond.

The CATF adopted the following scenario to guide their work:

An organized cyber disruption disables or impairs the integrity of multiple control systems, or intruders take operating control of portions of the bulk power system such that generation or transmission system are damaged or operated improperly.

1. Transmission Operators report unexplained and persistent breaker operation that occurs across a wide geographic area (i.e., within state/province and neighboring state/province).
2. Communications are disrupted, disabling Transmission Operator voice and data with half their neighbors, their Reliability Coordinator, and Balancing Authority.
3. Loss of load and generation causes widespread bulk power system instability, and system collapse within state/province and neighboring state(s)/province(s). Portions of the bulk power system remain operational.
4. Blackouts in several regions disrupt electricity supply to several million people.

Enhancing Resilience

"Resilience" is generally defined as the ability to recover or adjust to misfortune or change. More specifically, the ASIS SPC.1-2009 standard on Organizational Resilience[6] defines, "Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event." In recent years, in the context of strategies needed to enhance the reliable operation of critical infrastructures, resilience has come to be valued as much as protection. But what exactly is meant by resilient critical infrastructures? How is resilience measured and how much is needed?

Infrastructure Resilience

Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

[5] E.g., Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator

[6] ASIS SPC.1-2009, http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf

In October 2010, a study group[7] of the National Infrastructure Advisory Council issued its report "A Framework for Establishing Critical Infrastructure Resilience Goals[8]". The report provides a broader construct for resilience originally conceived by resilience expert Stephen Flynn. The construct is based on four features organized in a sequence of events prior to, during, and after a severe emergency event.

NERC's Severe Impact Resilience Task Force[9] has proposed a number of recommendations and considerations from the perspective of the reliable operation of the bulk power system, regardless of the cause of the emergency event. The CATF has focused its efforts on the measures that can be taken to prevent, deter, detect, and respond to a coordinated cyber attack from the perspective of the assets, systems, and networks used to monitor, operate and control the bulk power system such as Supervisory Control and Data Acquisition (SCADA), energy management systems (EMS), and generation management systems (GMS).

[7] The NIAC Study Group included a number of representatives from the electricity industry, including several members of the Electricity Sub-sector Coordinating Council.

[8] Ref. http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf

[9] Ref. report *Severe Impact Resilience: Considerations and Recommendations* http://www.nerc.com/filez/sirtf.html

Key Recommendations

The CATF has considered what aspects of cybersecurity would be particularly challenged through a coordinated cyber attack and considered options to protect the assets, systems, and networks that are critical to the reliable operation of the bulk power system. The following summarizes the key recommendations of this report that are described in the body of the report in further detail. While some of the recommendations identify areas that require further study coordinated through NERC's Technical Committees, others recommend that entities take certain actions to enhance their ability to prevent, deter, detect, and respond to a coordinated cyber attack.

1. **Continue Work on Attack Trees** – A separate working group under NERC's Critical Infrastructure Protection Committee (CIPC) should be established to further develop attack trees with the goal of populating the nodes, performing detailed analysis, and providing recommendations to industry from this analysis.

Prevent Deter	Detect	Respond
✔		

2. **Continue to Develop Security and Operations Staff Skills to Address Increasingly Sophisticated Cyber Threats** – Entities should develop strategies to attract cybersecurity talent and further develop the knowledge, skills, and abilities of existing staff to address increasingly sophisticated cyber threats and technology challenges that accompany grid modernization efforts.

Prevent Deter	Detect	Respond
✔	✔	

3. **Augment Operator Training with Cyber Attack Scenarios** – Several cyber attack scenario templates are included in Appendix C of this report. Entities should consider enhancing training to incorporate cyber attacks that raise operator awareness for a coordinated cyber attack.

Prevent Deter	Detect	Respond
	✔	✔

4. **Conservative Operations** – The *Severe Impact Resilience: Considerations and Recommendations* report prepared by the Severe Impact Resilience Task Force offers a number of recommendations regarding conservative operations. Entities should review this report and consider the practices that would apply to a coordinated cyber attack scenario.

Prevent Deter	Detect	Respond
		✔

5. **Conduct Transmission Planning Exercise** – Working with Department of Energy's national labs and a pilot group of electricity utilities, a transmission planning exercise should be coordinated by NERC to simulate a coordinated cyber attack that creates a cascading event and blackout. The event should attempt to

Prevent Deter	Detect	Respond
✔		✔

identify the point at which current transmission planning criteria is exceeded and allow for dynamic resilience and mitigation exercise.

6. **Continue to Endorse Existing NERC Initiatives That Help Entities Prepare for and Respond to a Cyber Attack –** Entities should consider greater participation and support of NERC's initiatives that can help the industry with cyber attack identification, defense, and response. Three examples are**:**

Prevent Deter	Detect	Respond
✔		✔

   - Cyber Readiness Preparedness Assessments (CRPA)
   - NERC Grid Security Exercise
   - ES-ISAC portal and collaboration

7. **Increase Awareness for Department of Energy Initiatives –** The Energy Sector Control Systems Working Group recently released the *Roadmap to Achieve Energy Delivery System Cybersecurity*. NERC's Critical Infrastructure Protection Committee should review these initiatives and support further development and implementation of these initiatives to help ensure protection of critical systems supporting bulk power system.

Prevent Deter	Detect	Respond
✔		

8. **Continue to Extend Public / Private Partnership –** Entities should review their cyber incident response plans to ensure an appropriate mix of operational, security, technical, and managerial staff are aware of how they need to evaluate, respond, and make timely decisions to slow or stop a coordinated cyber attack. This could include participating in ES-ISAC and government sponsored programs to share security-sensitive or classified information regarding cyber threats and vulnerabilities. In the event standard information sharing protocols are unavailable (e.g. between utilities, ES-ISAC, etc), alternative methods need to be defined.

Prevent Deter	Detect	Respond
		✔

Introduction

A highly coordinated and structured cyber, physical, or blended attack on the bulk power system, could result in long-term, difficult to repair damage to key system components in multiple simultaneous or near-simultaneous strikes. Unlike "traditional," probabilistic threats (i.e. severe weather, human error, and equipment failure), a coordinated attack would involve an intelligent adversary with the capability to bring the system outside the protection provided by current planning and operating practices. An outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods.

Security practitioners have always found it difficult to provide convincing demonstrations that the countermeasures they deploy are effective in preventing an attack. It is fundamentally difficult to provide conclusive proof of why an event did not happen.

Though no such attack has been successfully executed to date on the North American grid, the bulk power system remains an attractive target for acts of both physical and cyber terrorism. Goals of these adversaries are wide-ranging and could involve extortion, societal damage, and, in the case of state-sponsored attacks, acts of war.[10]

The purpose of the Cyber Attack Task Force (CATF) is to consider the impact of a coordinated cyber attack on the reliable operation of the bulk power system, and identify opportunities to enhance existing protection, resilience, and recovery capabilities.[11]

Approach

The scenario itself allows for a consequence driven approach. The premise is that the outcome of the attack has unacceptable consequences. It is impossible to consider and evaluate every type of risk to the bulk power system. As a result, we focus on the risks that matter as defined by consequences.

To address the objectives and goals the task force utilized a combination of industry expertise (both IT and operational), discussions with federal agencies and law enforcement, and incorporated lessons learned from current and past initiatives.

In addition, the task force attempted to capture and catalog different attack paths that could be utilized to create specific results from the given scenario. In other words, leverage intelligence from the community of interest to define what a coordinated attack would look like. We started to capture the many steps associated with different attack paths in what is called an Attack Tree.

Security practitioners have always found it difficult to provide convincing demonstrations that the countermeasures they deploy are effective in preventing an attack. It is fundamentally

[10] High-Impact Low-Frequency Event Risk to the North America Bulk Power System (June 2010)

[11] NERC Scope – Cyber Attack Task Force

difficult to provide conclusive proof of why an event did not happen. This is one of the reasons that the task force did not focus on the adequacy of the NERC CIP standards to prevent a coordinated cyber attack. Instead the task force included references to the CIP standards, both approved and under development, along with other tools, processes and recognized standards and guidelines from ISA and NIST as part of the industry's defensive capabilities to combat a coordinated attack. This problem is exacerbated further when dealing with unprecedented or infrequent events. Yet the threat environment going forward is likely to demand and feature a capability to prevent attacks or mitigate their impacts through coordinated response and effective information sharing.

Attack Trees are constructed from the point of view of the adversary. Creating good Attack Trees requires "*we think like an attacker".* The task force did not focus on how to defend a utility's systems when the model was originally started. Instead the task force thought about what an attacker wants to achieve and ways to accomplish it. In this case, the attacker wants to achieve blackouts in several regions disrupting distribution supply to several million people[12]. This approach was useful as those engaged for the project have a very good understanding of the mechanics associated with the elements required to severely impact the bulk power system.

One of the constraints encountered by the task force is the sensitivity of the information being gathered and determining a way to translate from sensitive to public so the larger industry can benefit from subject matter expert recommendations. This situation manifested itself on numerous occasions from discussions with law enforcement and the intelligence community on threat actor capabilities to detailed steps captured in the Attack Trees.

[12] Ingoldsby, Terrance R., 2010 Amenza Technologies Limited: Attack Tree-based Threat Risk Analysis, page 2

Adversaries, Motivations, and Capabilities

In the cyber realm, the ability to climb the line of consequences versus likelihood is very different than physical risks. The resources and requirements to execute an attack that can cause a catastrophic effect are much more available, and is really a matter of how an adversary chooses to manifest attack type or target selection. Attacker sophistication should be measured less in technical "craft" skills and more in terms of intent fitted to environment. Disrupting or hijacking system resources is one thing….destroying trust and confidence by poisoning data or compromising privacy information is another. [13]

The defense against a cyber attack scenario will include physical as well as cyber-based elements, some procedural and others involving strategic investments in physical infrastructure, capabilities, spares, and training.

There are a variety of interventions or attacks that adversaries might contemplate and each carries unique defensive planning and resource requirements. A holistic, tailored defensive posture prioritizes and balances these to achieve the optimal cost/benefit value delivery for the defender. The defense against a cyber attack scenario will include physical as well as cyber-based elements, some procedural and others involving strategic investments in physical infrastructure, capabilities, spares, and training.

There does not appear to be a universally accepted classification or grouping of advisories. Work done by the FBI, DHS, NERC, and security consulting groups with many years of experience do not all agree what the threat actor categories should be. In this report you will see references to Groups 1-3; High, Medium and Low Threat Actors; Criminals, Hackers, Hacktivists, Nation States, Organized Crime, Structured Criminals, Terrorists, and Foreign States. As you read about these groups from the different sources, the focus should be on intent and capabilities to conduct a coordinated cyber attack on the bulk power system. But also recognize that intent and capabilities can change very quickly.

Training offered as part of the Department of Homeland Security's Control System Security Program (CSSP) discusses three categories of threat actors: Group 1 Main Stream Threats, Group 2 Organized Threats, and Group 3 Terrorist and Nation State Threats

Group 1 is the largest threat group although they are typically not organized. These types of threats often compete for notoriety, fame, or personal research and members of this group can be anyone. There is some element of minor organization in this group, but historically the members of this group are lone actors. Often, as they become better known, and there is an increase in the demand for their services, both legal and illegal, their activity increases. It needs to be understood that there are capabilities within this group that can be used in the activities performed by group 2 and group 3 threat actors. Just because group 1 actors are not organized

[13] Likelihood and Consequences Chart – Mike Assante 2011

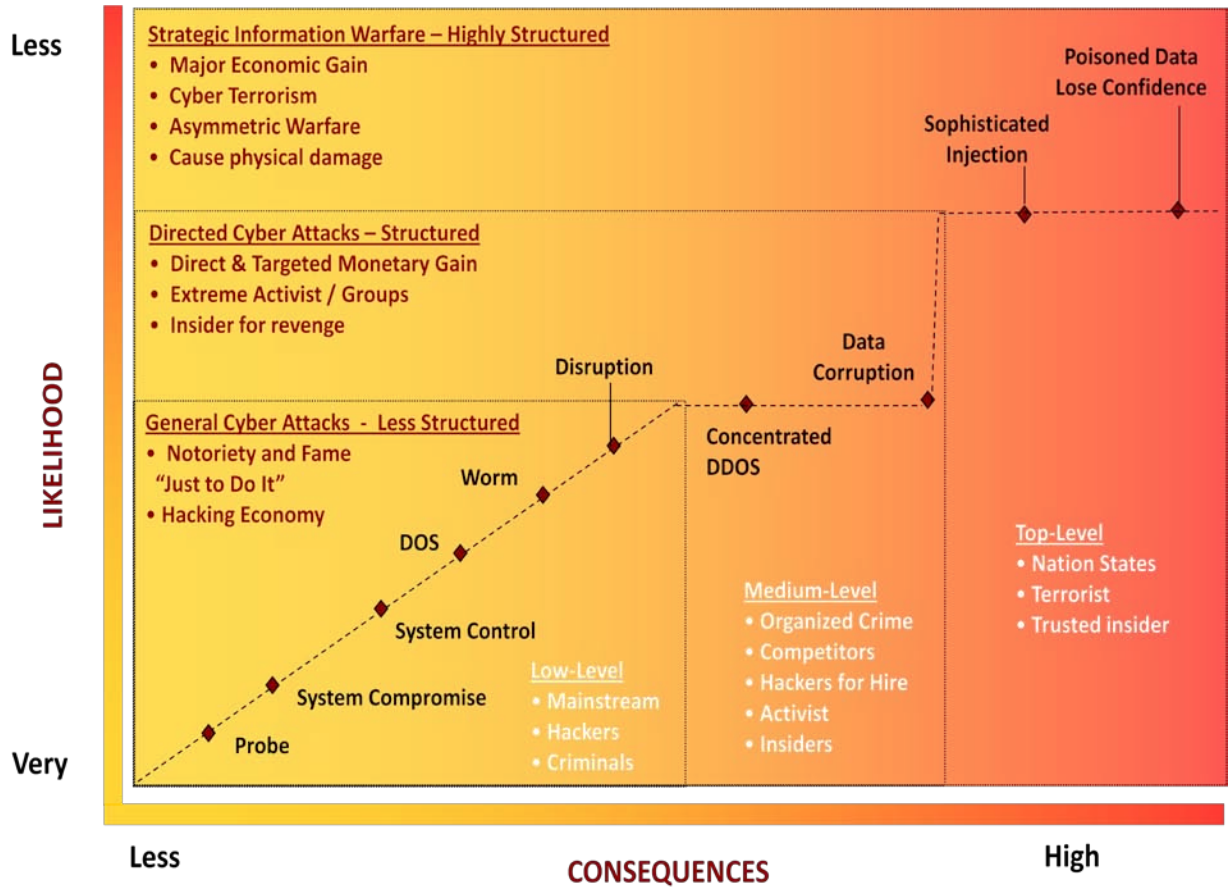
in numbers, and may not have a specific modus operandi or methodology, there is a good chance that unique capabilities exist that could be very useful in group 2 and group 3 activities.

Group 2 are more organized, and it is the organizational aspect that is cause for concern. By having a structure, this group can have membership elements that are diversified across a very large area, and may have access to disparate information systems that would normally be only accessible by a single actor. Often, collective intelligence is pooled together by group 2 members to help shape more effective and efficient attack strategies. Group 2 threats are most likely to develop specific target folders and use the information in those folders to plan, test, and perform targeted attacks.

The motivation for these attacks can be quite diversified, but it is generally observed that these attacks involve group level efforts supporting a common cause. Group 2 typically target a particular group or groups, and their motivation may be financial, revenge, theft of trade secrets or drawing attention to a cause (hacktivists). The capabilities in group 2 would be found useful in group 3 type activities, as group 2 factors often aggregate tools and methods to be more powerful. The end state of this aggregation may be attractive to group 3 actors (depending, of course, on what the goals are). Their attacks are more structured and sophisticated than group 1 attacks, but group 2 attacks often incorporate methods used by group 1. This would be expected considering that the attack lifecycle of target acquisition, system penetration, privilege escalation, and covert action is fairly ubiquitous across all group activities.

Group 3, asymmetric threats (often associated with terrorist or nation state), occurs when two forces of disproportionate size and capability are engaged in conflict. The goal of these types of attacks is to disrupt, terrorize or eliminate major aspects of society. Targets include financial institutions, political establishments, military organizations, and media outlets. Organizations involved in national security activities are also concerned about critical infrastructure, and how such threats could launch debilitating cyber attacks that include an impact on restoration and reconstitution activities. In addition to asymmetric threats, nation states that may have well-funded cyber warfare programs are also a concern.

Both asymmetric and nation state threats have significantly more resources than group 1 and 2 threats and as a result they can launch very sophisticated attacks. However, it should be understood that it is not unlikely for a group 3 actor to utilize tools, techniques, and procedures used by either group 1 or group 2. This reasoning could be extended to suggest that, when possible, group 3 actors will recruit the services of group 1 and 2 thread elements and capabilities. The impact or consequences of group 3’s attack could be catastrophic.



The risk equation that is often most appropriate for critical infrastructure is one that involves threat, vulnerabilities, and consequence. Using what are commonly known as 'threat curves', we can plot different types of threats and their associated elements against the likelihood of such activities happening. In its simplest form, we can plot consequence against likelihood and then plot the activities of the three types of groups discussed earlier.

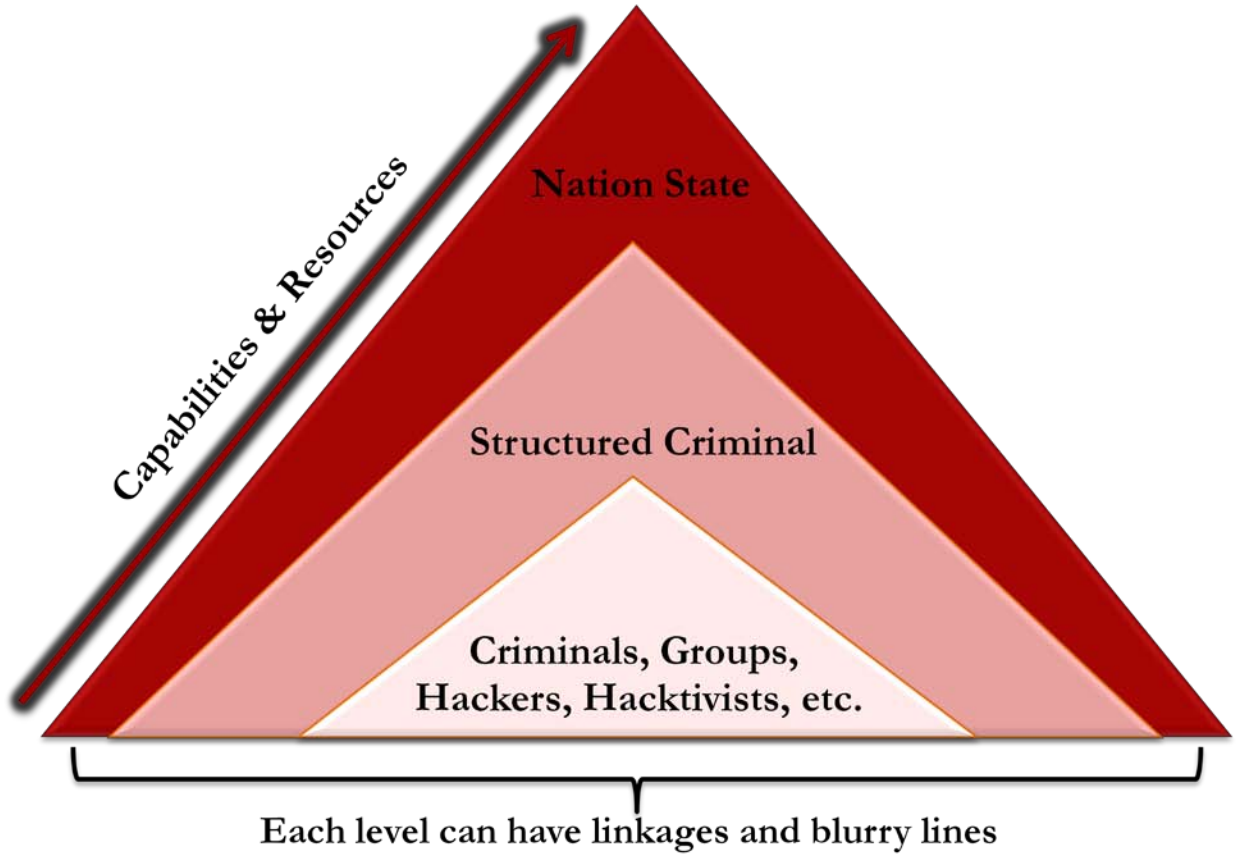
We notice from the graphic that the more benign activities would occur in the bottom left-hand corner of the graph with the most critical actions or consequences in the upper right. As the plot moves towards the top, the top right-hand element of the curve is referred to as the 'high impact low frequency' domain. This is the area of the graph containing the most severe consequences.

But looking at the way the curve starts in the bottom left-hand corner, we can see how the strategies of the group 1 actor curve up into the right. This is because we anticipate that the activities being performed in an attempt to generate greater consequence become more difficult to accomplish. Taking into consideration that group 1 type actors are usually lone actors, and if they do exist in small groups there is limited organization, the level of effort increases noticeably as they try to increase their attack complexity. This is not necessarily true if the lone actor is an insider. See the reference to insiders later in this document.

The curve flattens when it gets to the group 2 domain, the primary reason being that the characteristics of group 2 suggest that the organization and the cultural make up of the group

will have an ability to increase consequences without necessarily having any less likelihood of success. The reasons for this are many, but can include the fact that the group 2 structure facilitates for advanced reconnaissance and the development of target folders which would be used specifically to ensure there is enough intelligence to ensure successful attack. Group 2 may use elements and perhaps membership from group 1, but the motivations of group 2 combined with an advanced and collaborative technical capability results in an increase in consequence with no deterioration likelihood for success.

Lastly, group 3 is assumed to have very specific goals and intentions with regards to consequence. As these consequences are desired to be extreme, such as widespread economic impact and the degradation of recovery capabilities, the level of effort is significant. The interesting thing about group 3 activities in the high impact low frequency domain is that we could expect well-planned and well-funded cyber attacks to have cascading effects across critical infrastructure elements. Currently, there is an abundance of available information suggesting that national critical infrastructures have significant interdependencies and interconnectedness. The 2003 Blackout illustrated the interdependencies of critical infrastructure, and showcased how a catastrophic failure in one specific sector has extremely far-reaching results in others.



Low Level Threat

Criminals, Hackers, Hacktivists

- Can be less experienced
- Limited financial resources
- Opportunistic in nature
- Target known vulnerabilities
- Use packaged attack tools
- Can be motivated by bragging rights, theft, activism, and exploration
- Market provided defenses are usually effective

Medium Level Threat

Structured Criminal

- Can be experienced and skilled
- Access to financial resources
- Targeted in their attacks
- Posses objectives
- Use a range of attack tools
- Can be detected
- Exploit known vulnerabilities very quickly

High Level Threat

Nation State

- Draw upon skilled people
- Demonstrate sophisticated tactics
- Deep financial resources
- Rely on recon and planning
- Target specific technologies & data
- Develop customized attacked tools
- Can exploit unknown vulnerabilities
- Well defined goals & objectives Difficult to detect & remove
- Can use insider access
- Access to supply chains

Attacker capabilities vary greatly based on skill level and resources. High Level Threat Actors have the capability to employ or exploit all of the following:

Network traffic capture and analysis
Intercept and modify data inputs and outputs
Inject values or data into bidirectional traffic (Man-In-The-Middle attacks)
Physical layer (tampering, inputs, and add-ons)
Data & datalink layer (MAC address spoofing, root bridge, enable unauthorized DHCP server, VLAN trunking, etc.)
Network layer (injecting blackhole, rerouting, route manipulation, inject packets and malformed packets, source route IP packets, etc.)
Application layer (DNS cache poisoning, web browser attacks, digital certificate impersonation, TCP session hijacks, injects)
System layer (Operating System attacks, privilege escalation, remote control, computer resource management, etc.)
Behavioral (people) layer (man-to-machine interface and process)
Compromising and owning a connected device with administrative privileges
Denial of service attacks (Complete, Selective, etc.)
Weak authentication/authorization
Buffer Overflows
Integer Over/Underruns
Format String Flaws
Use of fuzzers and other logic flaws
Operating System and application flaws (evaluate common code weaknesses/programming errors and IT vulnerabilities)
Connected devices, servers, and databases (injection attacks)
Access to computer resource management (the actual board)
Consider the process for updates (supply chain, vendor patches)[14]

Recent work by the FBI has classified threat groups into six major categories with references to methods of reaching their goal. Cyber Network Exploitation (CNE) is considered non-destructive while Cyber Network Attack (CNA) is destructive. CNE activity could be part of a long term effort to amass CNA capabilities with kinetic impacts, or generate new novel techniques, tactics, and procedures.

CNE may include expansion of threat actor understanding. CNE may also increase future CNA capability. For example, CNE in the form of exfiltration may be non-destructive in the present, but crucial to future destructive CNA capabilities or power projection.

CNA could be conducted as a means to an end in isolation, or as part of a larger, more complex effort to achieve broader goals beyond the effects of its own specific kinetic impacts. For example, CNA goals could extend to creating policy movement or fear among governments or populations.

[14] Scipio Group, LLC 2011

Cyber Threat Group	Primary Motivation	What They Want	How They Get It
Foreign State	National Interest Warfare	Information Control	CNE CNA
Terrorists	Ideology	Attention	CNA
Criminal	Money	Personally Identifiable Information Ransom	CNE CNA
Hacker	Personal Interest	Methods	CNE
Hacktivist	Cause	Support	CNA
Insider	Anger Personal Enrichment	Revenge Information	CNA CNE[15]

Insiders

Insiders pose the greatest threat, especially if they are working with a Foreign State or other High Level Threat Actors, because of their detailed knowledge of system operations and security practices. In addition, they have legitimate physical and electronic access to key systems and the controls designed to protect them. Insider individuals can provide qualitative, technical or physical assistance to the team requirements of sophisticated adversaries or pose a unique unilateral threat detection challenge, if acting alone.

Individuals with the highest level of access pose the greatest threat. Furthermore, an individual with access to grid infrastructure could unwittingly or inadvertently introduce malware into a system through portable media or by falling victim to social engineering e-mails or other forms of communication.[16]

[15] FBI Presentation, NERC CIPC meeting, September 14, 2011, "US Electricity Sector Faces High Cyber Exploitation Threat, Low Cyber Attack Threat

[16] Department of Homeland Security Office of Intelligence and Analysis Note – Insider Threat to Utilities

What a Coordinated Attack Looks Like

Depending on the capability and intent of an attacker, it can be very difficult to determine in advance that a coordinated cyber attack is occurring. A sophisticated attack, such as the Stuxnet worm, could have some or all of the following characteristics:

- First seen (new type of attack) or very rare
- Requires resources & skill to develop (thousands of hours of planning, development, and testing
- Usually highly structured threat actors
- Can be specific & directed
  - Technology (hardware) targeted
  - Application (software) targeted
  - Objective-based (e.g. impact BPS reliability)
- Can contain counters or responses to neutralize anticipated protective measures
- Difficult to attribute
- High reliability (usually tested before use)[17]

Cyber attack paths and methods (i.e. attack vectors) can also vary significantly based on the capability of the attacker, resource constraints, the intended target, and consequence. Attack vectors include:

- Via communication link between data and decision layers (e.g. Historian or real-time database server)
- Via connected WAN (e.g. Transmission SCADA Network, Corporate Network, etc.)
- Via connected device (e.g. Travel upstream from a data concentrator or application server)
- Via telecommunication network (e.g. POTS into dial-up accessible equipment)
- Via Wireless network (e.g. Blue tooth, 802.11x, etc.)
- Via remote connection (e.g. VPN for maintenance)
- Via portable media (e.g. USB stick)
- Physical access to the system[18]

A coordinated cyber attack may be timed to coincide with routine or abnormal bulk power system wide operational vulnerability periods in the daily or seasonal Demand-Response cycle. Cyber attacks may be combined with physical attacks which might be used to soften the system for a cyber knockout punch or to gain access to key facilities.

[17] Scipio Group, LLC 2011
[18] Ibid

Prerequisites of an Attack

Three conditions must be present in order for an attacker (also known as a *threat agent*) to carry out an attack against a utility's system.

1. The defender must have **vulnerabilities** or weaknesses in their system.
2. The attacker must have sufficient **resources** available to exploit the defender's vulnerabilities. This is known as **capability.**
3. The attacker must believe they will **benefit** by performing the attack. The expectation of benefit drives **motivation**.

Condition one is completely dependent on the utility. Whether condition two is satisfied depends on both the utility and the attacker. The utility has some influence over which vulnerabilities exist and what level of resources will be required to exploit them. Different attackers have different capabilities.[19]

Condition three is associated with intent. Does the attacker have intent to disrupt or destroy the target or to exploit the target without disruptions?

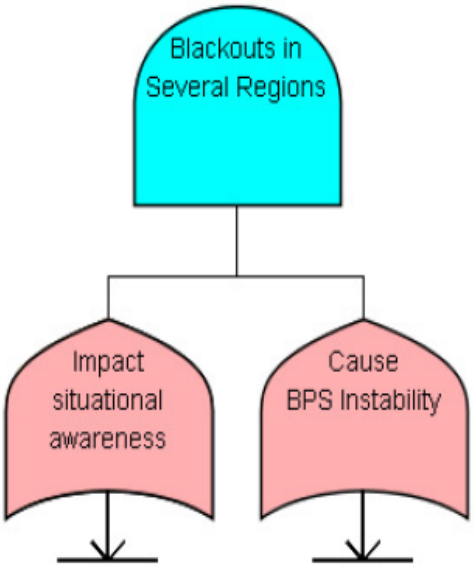
The task force chose to use an attack tree methodology to begin to build a picture of what a coordinated cyber attack could look like based on the attacker's intent to disrupt.

Attack Trees allow you to incorporate the capabilities of the attacker using specific profiles. The task force created attacker profiles that corresponded to low, medium, and high threat levels. In addition, resources (i.e. technical capability, noticeability, cost of attack, and attributability) associated with each leaf on the tree can be pruned or eliminated based on the profile of the attacker. In other words, an attacker with only medium technical ability would not be able to successfully navigate certain attack paths because steps (leaf nodes) required strong technical capabilities.

See Appendix A for an overview of attack trees.

[19] Ibid, page 3

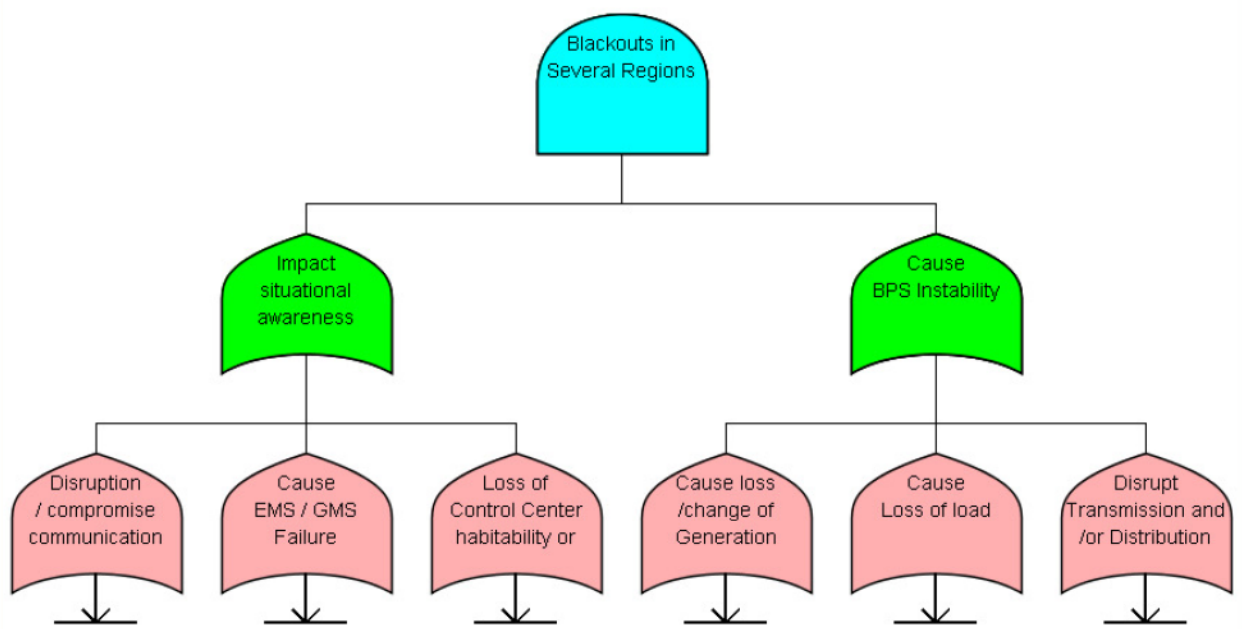
Coordinated Cyber Attack Scenario and Assumptions:



1. BPS Instability - Transmission Operators report unexplained and persistent breaker operation that occurs across a wide geographic area (i.e. within state/province and neighboring state(s)/province(s).)
2. Impact Situational Awareness - Communications are disrupted, disabling Transmission Operator voice and data with half their neighbors, their Reliability Coordinator, and Balancing Authority.
3. BPS Instability - Loss of load and generation causes widespread BPS instability, and system collapse within state/province and neighboring state(s)/province(s). Portions of the grid remain operational.
4. Attack Result - Blackouts in several regions disrupt distribution supply to several million people.

The foundation assumption for a successful attack that results in a blackout in several regions is that two events need to occur: 1) situational awareness needs to have been compromised and 2) there must be a bulk power system event or instability.

Operational events regularly occur on the bulk power system without any noticeable impact to consumers. Operators are trained to take actions to mitigate the impact of such events. However, if the operator is unaware of wide area operating conditions, he/she can't implement mitigation actions and the result can be significant.



Expanding each of the two events:

Situational Awareness is impacted IF

- There is a Disruption / Compromise in Communications OR
- There is a failure of the Energy Management System or Generation Management System OR
- The Control Center is inaccessible or uninhabitable

The BPS Instability can occur IF

- There is a Loss/Change in Generation OR
- A Loss of Load OR
- A Disruption to Transmission or Distribution

Beyond the second layer of the Attack Tree are multiple layers that expand into literally millions of steps and paths (nodes) to accomplish the attacker's intent – blackouts in several regions. Work continues in the development of comprehensive attack trees and is the subject of a task force recommendation.

Detection Capabilities

The ability to respond to an attack is contingent on the utility knowing that the attack could occur, is occurring or has occurred. The earlier the alert or warning, the better the chances that the operator, security teams and response tools can implement mitigation measures to minimize the impact of the attack on the bulk power system. However, operators can only go to the fight with the tools, awareness and training they have, so the effectiveness of mitigation depends critically on strategic preparations and investments necessarily taken over a long period of time at significant expense.

Operators must also be cognizant that the attacker may adapt to the implementation of defensive measures. But detection allows system defenders to manage the situation and make decisions to limit consequences or increase the effort required by the attacker throughout the process.

Operators must also be cognizant that the attacker may adapt to the implementation of defensive measures. But detection allows system defenders to manage the situation and make decisions to limit consequences or increase the effort required by the attacker throughout the process.

Coordinated attacks require a significant amount of planning. Consequently, indicators of an attack could be identified far outside the operator's normal field of vision. Indicators could occur at a neighboring utility, within a balancing authority, in another region or interconnect or even in another country. Indicators may arise in areas totally outside the electricity sector, such as in the finance, IT or communications sectors.

Monitoring information sources for indicators of an attack is essential to maintaining situational awareness. Effective sector information sharing is key to obtaining useful indicators and warnings of a cyber attack and bulk power system risk.

An important nexus for collaborative information sharing on threats, vulnerabilities, prevention, and mitigation is the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Operated by NERC, ES-ISAC is a center for sector-wide cybersecurity coordination, trust, and engagement. This vision is achieved through rapid sharing and analysis of information with the sector and its partners, providing sector-wide visibility and situational awareness. ES-ISAC staff are integrated with activities of the National Cybersecurity and Communications Center (NCCIC), a major government fusion cell operated by Department of Homeland Security (DHS).

In the event an attack, disables the ES-ISAC's ability to communicate with the electricity sector, a backup plan for distribution of critical information would need to be established. This is part of NERC's Crisis Plan, which is still under development. This is also true for inter-utility communication.

Global Monitoring of Internet Activity

A number of security firms and IT service providers have sensors on sections of the Internet and for a fee will provide analysis of a company's network traffic offering alerts and indicators of potential attacks or reconnaissance.

In addition, some utilities have established partnerships with IT service providers to share advanced threat information. Some of these service providers also work with Department of Defense information, and can take advantage of other information sharing sources such as the DoD Cyber Crime Center's DIBNet. For example, Lockheed Martin announced a program called Palisade intended to provide utility and energy industry IT analysts with advanced threat detection and forensic tools, actionable intelligence to effectively identify and mitigate cyber security threats.[20]

Federal Initiatives

Several federal agencies have initiatives in progress that are designed to assist the electricity sector in identifying indicators of a coordinated attack

- Department of Energy's Electricity Sector Network Monitoring (ESNM) program coordinated with Pacific Northwest National Laboratory (PNNL).
- The Department of Defense's program with Defense Industrial Base companies and their Internet Service Providers. DoD is providing attack signatures to help identify potential attackers. This program is expected to expand into the electricity sector.
- Department of Homeland Security - The Einstein system is intended to provide the government with early warnings about cyber attacks against federal networks, near real-time identification of malicious attacks, and automated disruptions of those strikes. The first version of Einstein dates back to 2003 and the second phase rolled out in 2008. It is now deployed at 15 out of 19 departments and agencies and in 2010, Einstein 2 sensors picked up 4.5 million "hits" or alerts based on pre-determined intrusion detection signatures. The Department of Homeland Security is currently working on Einstein 3, "which will provide DHS with the ability to automatically detect and disrupt malicious activity before harm is done to critical networks and systems."

While these types of programs for monitoring and identification of attacks have a solid foundation, there are limitations. Attacks can be crafted and implemented where there are no observable signatures in place.

Peer Groups

NESCO, working with the National Electric Sector Cybersecurity Organization Resource (NESCOR), serves as a focal point bringing together utilities, federal agencies, regulators, researchers, and academics. This group, along with domestic and international experts, developers, and users help to focus cybersecurity research and development priorities, to identify and disseminate effective common practices, organize the collection, analysis and

[20] http://s1.securityweek.com/lockheed-martin-launches-cyber-security-solution-utility-and-energy-industry

dissemination of infrastructure vulnerabilities, and threats. NESCO works to identify and support efforts to enhance cybersecurity of the electric infrastructure. This project is being partially funded by the Department of Energy.

NESCO has established interest groups associated with intrusion detection, security architecture, threat assessment, and forensics.

The Electric Power Research Institute (EPRI) is coordinating several complimentary initiatives associated with industry and federal agencies. These efforts include 1) assessing combined cyber-physical attacks where the deliverables involve attack scenarios to feed into risk assessment models; 2) creating a scalable Advanced Metering Infrastructure (AMI) Incident response. The intent is a logical architecture for a scalable AMI intrusion detection system, a set of alarms and alerts to be standardized across vendors and guidelines for responding to AMI alarms.

A number of utilities have informal information sharing arrangements so sensitive information can be communicated to trusted sources.

Alerts

There are multiple sources of alert information that the electric industry can reference to better identify early signs of a coordinated cyber attack. NERC's ES-ISAC and DHS's Industrial Control System – Computer Emergency Response Team (ICS-CERT) are import providers of relevant threat and vulnerability information related to Industrial Control Systems.

Many software and hardware manufacturers have e-mail or other alert distribution methods to notify customers of vulnerabilities and associated mitigation measures.

In addition to software and hardware vendors, utilities can look to activity in other countries as a potential precursor to a coordinated attack in North America.

Specialized Industrial Control Systems software along with off-the-shelf software is utilized in other critical infrastructure sectors that have close ties to the electricity sector. For example, PLCs are used in oil and nature gas and water facilities as well as power stations. Monitoring for malicious activity in other sectors can be an early indicator of a coordinated attack in the electricity sector.

See Appendix B for a list of sources and associated links.

Precursors and Local Indicators

Experienced operators and support staff usually develop a 6th sense in regards to their job. Many times it is this "feeling" that something isn't right that heads off larger problems. While using this 6th sense is certainly valuable, establishing a baseline of expected values and then comparing those against real-time data points is an excellent method of comparison to determine if an unexpected situation exists. Following anomaly detection, trained staff can then follow-up with detailed analysis.

Appendix F contains a list that can be used as a starting point for indications of an unusual event. By developing real-time monitoring for these key metrics and comparing them to the base line, potential cyber attacks could be identified. However, these indicators do not take into consideration loss of data integrity where values are still within tolerances established by the entity. The industry eventually needs security state monitoring tools that trigger autonomic (i.e., quick device response) and/or dynamic (i.e., can evolve) corrective actions within the control system, while allowing operators to override them, if necessary[21] One potential proxy for this type of capability is the North American Synchro Phasor Initiative.

Synchrophasors are precise grid measurements now available from monitors called phasor measurement units (PMUs). PMU measurements are taken at high speed (typically 30 observations per second – compared to one every four seconds using conventional technology). Each measurement is time-stamped according to a common time reference. Time stamping allows synchrophasors from different utilities to be time-aligned (or "synchronized") and combined together providing a precise and comprehensive view of the entire interconnection. Synchrophasors enable a better indication of grid stress, and can be used to trigger corrective actions to maintain reliability (i.e. improving situational awareness)[22].

This type of technology provides indication of electrical network issues and could be used as an early warning indicator on a large scale. However, due to the speed of cascading events whether man-made or natural and their PMU indication, response to this type of detection may need to be automatic using predefined programmatic actions.

[21] Roadmap to Achieve Energy Delivery Systems Cybersecurity – September 2011, page 29

[22] North American Synchro Phasor Initiative - https://www.naspi.org/

Deterrence / Defensive Capabilities

In broad terms, we can envision protecting the electricity sector with three separable, but complementary, layers of capability. The first layer is deterrence—capabilities and policies designed to convince an adversary not to launch a cyber attack. This is the job of the U.S., Canadian and Mexican governments. The second layer is defense—capabilities designed to reduce the effectiveness of the adversary's cyber attack. This layer is a primarily the responsibility of the electricity sector asset owners but does include governmental assistance. The third layer is reconstitution and robustness—capabilities designed to enable the bulk power system to continue functioning once it has suffered cyber damage and to enable the electricity sector to restore and rebuild its infrastructure after being damaged. Again, this is primarily the responsibility of the asset owners.

These layers achieve their objectives in different ways. Deterrence influences the adversary's intentions, convincing an adversary not to attack; defense works against the adversary's capabilities, defeating attacks that the adversary launches; reconstitution and robustness reduce the implications of successful attacks by the adversary. The layers complement each other by making up for limitations in other layers. If deterrence were known to be perfect, defense and reconstitution would be unnecessary; similarly, if defense were perfect, deterrence and reconstitution would be unnecessary. But, when none of the layers is perfect, each contributes to the sector's overall ability to protect itself.

Deterrence is frequently divided into two types—deterrence by punishment and deterrence by denial. When relying on a strategy of deterrence by punishment, the U.S., Canadian, and Mexican governments threaten to inflict costs (i.e. punishment) in retaliation for the bulk power system being attacked. The effectiveness of deterrence by punishment depends on both the size of the costs being threatened and the credibility of the threat. Credibility depends on both the ability to retaliate and the will to retaliate.

Deterrence by denial works by a different logic: in this approach, the electricity sector deploys capabilities to convince its adversary that the probability of its attack succeeding are low; this reduces the expected benefits of the attack and can therefore result in successful deterrence.[23]

The scope of this document will focus on the electricity sector's defensive and reconstitution/ robustness (i.e. survivability) capabilities.

A defense in depth security architecture has been, and continues to be, the foundation entities rely on to defend against cyber attacks. However, the engineering design of the electrical system also provides redundancy and resiliency that can help in minimizing or slowing down the impact or progress of an attack.

The NERC Critical Infrastructure Protection standards, CIP002 – CIP009 version 3, provide a minimum level of control and protection for what an entity believes are their critical assets and

[23] Deterrence of Cyber Attacks and the U.S. National Security, Charles L. Glaser

associated critical cyber assets. Specific electronic and physical controls and processes are mandated for all critical cyber assets and any cyber assets within the defined electronic and physical security perimeters.

CIP-002 – CIP-009 Version 4, which has not been approved by FERC, and CIP-002 – CIP-011 Version 5, which is still under development seek to clarify the breadth of assets that should be protected to provide adequate resiliency to the BPS in response to cyber and physical attack.

Other well known standards and documents that serve to help entities protect their key assets include;

ANSI/ISA-99 is a complete security life-cycle program, with best practices for developing and deploying policy and technology solutions to address security issues in control systems. One aspect of the standard involves containing communication in control sub-systems to avoid having security issues in one area migrate to another area. ISA-99 introduces the concepts of "zones" and "conduits" as a way to segment and isolate the various sub-systems in a control system. A zone is defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence. Equipment in a zone has a security level capability. If that capability level is not equal to or higher than the requirement level, then extra security measures, such as implementing additional technology or policies, must be taken.

- **NIST SP800-53**, "Recommended Security Controls for Federal Information Systems," was developed primarily for Information Technology systems, but has been updated to address industrial control systems as well. It contains information for securing electronic systems from cyber intrusion. The standard is organized in sections or families of security categories.

- **NIST SP800-82**, "Guide to Industrial Control Systems (ICS) Security," is a guideline for securing industrial control systems. It is organized much the same as NIST SP800-53, but focuses on industrial control systems.

- **SANS 20 Critical Security Controls** - These Top 20 controls were agreed upon by a powerful consortium brought together by John Gilligan (previously CIO of the US Department of Energy and the U.S. Air Force) under the auspices of the Center for Strategic and International Studies. Members of the Consortium include NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities.

In addition to the CIP standards, NERC alerts (e.g. Aurora, Stuxnet, and other vulnerabilities) provide guidance on additional controls to protect vulnerable or at risk equipment from attack.

Appendix H contains a list of some common defensive capabilities that have been or could be employed by electric utilities as part of their overall defense in-depth security architecture.

Education / Training

As a coordinated attack has not been experienced to date, an operator faced with such an attack would have no real-life experience to draw on when responding to it. Further, little training presently exists to drill responses to these events, though certain organizations have recently begun to incorporate this material into their training programs.[24]

Training needs to include not only operators but field technicians as well. Focus should be on establishing a baseline to judge if "something looks or acts differently.".Then, the training needs to exercise the entities incident response plan which includes reporting.

Appendix C contains sample cyber attack scenarios that could be used to augment operational training.

More formal attacker/defender exercises such as those offered by Idaho National Laboratory (INL) are extremely beneficial in making entities aware of how attackers can respond.

NERC's Cyber Risk Preparedness Assessment (CRPA) is complementary to the program offered by INL. Using cyber threat and attack scenarios, this NERC-sponsored project conducts a qualitative, expert-based assessment of the preparedness of BPS entities to detect, respond to, and limit the potential damage caused by plausible cyber incidents.

These assessments focus on BPS entities' abilities to protect their cyber assets and improve preparedness regarding their cybersecurity posture. This is done by examining an entity's ability to defend its information systems, deter/deny attacks against those systems, detect attacks against its own or its peer systems, and respond to cyber attacks in a timely and efficient manner. The exercise also assesses the ability of BPS entities to isolate and limit attacks so that a system is able to withstand subsequent equipment losses and quickly be restored.

The objective is to leverage technically grounded cyber threat scenarios as the basis for assessing how BPS entities might detect, respond to, mitigate, and report cyber incidents, and to identify any capability gaps in their cybersecurity postures. In turn, this assessment will be used to identify steps required to improve overall BPS preparedness. [25]

Incident Response Plans

Many entities have existing emergency plans that can complement or provide a foundation for cyber incident response planning. CIP008 requires the establishment and testing of a cyber incident response plan on an annual basis. Some of these plans address NERC or Regional Transmission Operator (RTO) requirements to ensure operational continuity, so backup or redundant assets could be leveraged to provide on-going capabilities from an incident.

[24] High Impact, Low-Frequency Event Risk to the North American Bulk Power System, June 2010

[25] NERC Cyber Risk Preparedness Assessment – Tabletop Exercise Report April 2010

For example:

- NERC Reliability Standard EOP-005 requires a restoration plan to recover from a partial or total shutdown of the bulk power system. This plan would identify assets that would be utilized for such a recovery. The incident response plan could be enhanced to include processes for addressing cyber incidents affecting restoration plan assets.

- NERC Reliability Standard EOP-008 establishes requirements to ensure continued reliable operation of the BPS in the event of the loss of a primary control center. A cyber incident response plan could be enhanced to assess this loss from a cyber perspective and provide information to complement the loss of control center plan.

The Severe Impact Resilience: Considerations and Recommendations report created by the Severe Impact Resiliency Task Force contains recommendations to address the loss of both primary and backup control centers.

NERC Reliability Standard COM-001 establishes requirements for adequate and reliable telecommunications and operating information. Entities would establish levels of redundancy or resiliency (or both) and provide an operational plan to recover from a loss.

Incident response plans could define crucial planning materials to allow for smooth response activities. This includes defining accurate and precise roles and responsibilities between IT, operations, and other support teams. Listing potential options for containing an incident, suggested measures for removing a threat such as malware or compromised accounts, suggested forensic methods, escalation methods, third party notification procedures, including vendors and law enforcement.

Defining roles and responsibilities will assist in the escalation and mobilization of response activities. Clear delineations between teams should be defined. Additionally, particular individuals should have clear authority to make decisions surrounding investigation and response activities as well as recovery activities.

At the industry level, NERC is in the process of finalizing their Crisis Response Plan. At the national level is the National Response Framework (NRF). The National Response Framework presents the guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies – from the smallest incident to the largest catastrophe. This important document establishes a comprehensive, national, all-hazards approach to domestic incident response.

The framework defines the key principles, roles, and structures that organize the way we respond as a nation. It describes how communities, tribes, states, the federal government, private-sector, and nongovernmental partners apply these principles for a coordinated, effective national response. It also identifies special circumstances where the federal government exercises a larger role, including incidents where federal interests are involved and catastrophic incidents where a state would require significant support. The framework enables

first responders, decision-makers, and supporting entities to provide a unified national response.

Complimentary to the NRF is the DHS National Cyber Incident Response Plan (NCIRF). The National Cyber Incident Response Plan (NCIRP) was developed according to the principles outlined in the National Response Framework (NRF) and describes how the nation responds to significant cyber incidents.

ES-ISAC has developed a policy protected communications corridor which delineates special protections and handling for security discussions to encourage participation from the entities and insulate against excessive compliance concerns which might otherwise impede vital security dialogue. Policies like this set the stage for enhanced security by establishing venues for effective information sharing crucial to BPS risk management and response.

Rules of engagement for detecting, containing, and eradicating various incident scenarios will help guide personnel who are familiar with the incident response plan. This may include checklists for containment methods, procedures for forensic capture and evidence handling, and guidelines for disabling compromised accounts or reimaging server equipment.

One of the most important roles of any incident response plan involves communication. Communication could involve coordination:

- Between Reliability Coordinators
- Between Balancing Authorities
- Between Transmission Operators – minimize activities (i.e. maintenance outages) that would constrain an interface
- Between utilities
- With law enforcement
- With National Security Staff
- With regulators
- With ES-ISAC
- Between other sectors (oil and natural gas, nuclear, and dams)
- With and among technology vendor community participants

Creating an incident response plan is only one step towards being prepared for a security incident. It is invaluable to hold multi-team exercises or drills which develop familiarity with the incident response plans and defined roles and responsibilities during such events. Additionally, scenario-based drills which offer a plausible situation are a powerful tool to prepare staff on the potential confusion and hesitation which is inherent in an ongoing security incident. As part of any drill and in the case of an actual coordinated attack, it is imperative to communicate significant operational actions taken including their success or failure in mitigating or stopping the attack. This information is vital to partners so their responses are complimentary and not disruptive.

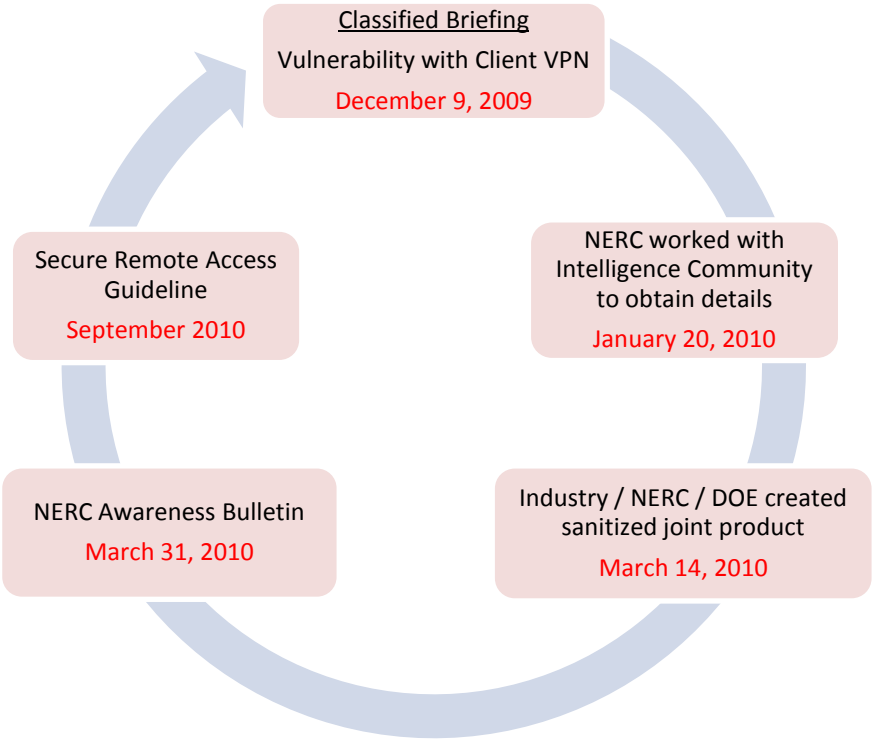
Auxiliary preparedness materials such as customer communication templates, emergency contact lists and preplanned secure/alternative communications methods (e.g. phone conference bridges; Government Emergency Telecommunications System (GETS) & Wireless Priority System (WPS) for priority access to telecommunications; satellite phone communications for the occurrence where landline and cellular facilities are not available) will enable a more rapid response operation. Creating customer communication templates may help customer support line representatives address calls from customers while other prepared documents may act as a template for communications staff to engage the local news media or government officials during or shortly after any impact from a security related incident. Emergency contact lists may list mobile contact information for management escalation and support staff such as operations staff, IT or cyber security team members. Additionally, it may list outside parties such as ES-ISAC, local, state or federal law enforcement, managed security service providers and system vendor technical support lines.

Information Sharing

Information sharing is a critical component of any preparation as well as part of the actual response plan. Besides the formal, regulatory requirements for reporting unusual events outlined in the NERC CIP standards and the Department of Energy's OE-417, there exists an informal communication network between utilities and non-regulatory entities such as the North American Transmission Forum and the North American Generation Forum.

There have been successes between the industry, regulatory agencies and the intelligence community with taking classified intelligence, having industry experts assess sensitive information in a classified setting, remove or translate sensitive data and create an alert that can be distributed to a wider audience in the electricity industry.

A case study of success:



This exercise of having industry experts work with NERC and the Intelligence Community demonstrates the process can work. Future team efforts should strive to reduce the amount of time from briefing to awareness/alert.

Existing formal and informal sources of information include: NERC ES-ISAC, RCIS / CIPIS, North American Transmission Forum, North American Generation Forum; US-CERT, ICS-CERT, RRO and RTO "communities" – mail distribution groups, newsletters, etc. and Vendor "User Communities" such as EMS users' groups.

Energy Security Public-Private Partnership (ES3P) Joint Working Group has been formed under the Electricity Sub-Sector Coordinating Council (ESCC) and the Energy Sector Government Coordinating Council (ES-GCC). With co-Chairs from Department of Energy and NERC, as well as representation from Departments of Defense and Homeland Security, industry trade groups and interdependent sectors (such as Oil and Natural Gas, Water, Nuclear), ES3P offers a protected venue for sensitive critical infrastructure and mission assurance discussion.

Gaining awareness of a cyber attack before it occurs and stopping its effects is the best case scenario for information sharing. Sharing of information during the attack's reconnaissance phase or early delivery phase will help achieve this end.

Sharing of concise indicators of compromise (IOC) or attempted compromise will allow for quicker analysis of information and development of mitigations to prevent future incidents. These indicators of compromise may take the form of file MD5 hashes, IP addresses, targeted

phishing email header information, captured network traffic, or other detailed activity. Such IOCs will be detected by the industry and must be shared with its various partners such as the ES-ISAC to 'connect the dots'. The correlation of related indicators of compromise reported from independent industry members will create an industry view of attacks and will lead to informed preventative and detective measures which reduce overall risk to the BPS.

Post-Event Analysis (Lessons Learned)

In order to properly prepare for the next security incident it is critical to capture lessons learned from prior incidents such as Stuxnet, Aurora, Night Dragon, Shady Rat and even events such as major hurricanes or tornados that resulted in disruptions. The lessons learned process should strive to identify how to prevent future attacks, prevent or limit disruption if they do occur, and create early visibility of such attacks through enhanced awareness and security monitoring.

Additionally, analysis of publicly disclosed attacks may provide a level of learning which may be incorporated into incident response plans, protective measures, resilience activity and preparedness. The FBI is working with the Pacific Northwest National Laboratory to evaluate and trend cases related to the electricity sector. The results of this analysis will be an important reference.

The NERC enterprise-wide event analysis program is based on the recognition that bulk power system events that occur, or have the potential to occur, have varying levels of significance. The manner in which registered entities, regional entities, and NERC evaluate and process these events is intended to reflect the significance of the event and/or specific system conditions germane to the reliability of the bulk power system and the circumstances involved.

The key ingredients of an effective post-event analysis program are to:

- Identify what transpired – sequence of events;
- Understand the causes of events;
- Understand the vulnerabilities that were exploited;
- Identify and ensure timely implementation of corrective actions;
- Develop and disseminate recommendations and valuable lessons learned to the industry to enhance operational performance and avoid repeat events;
- Develop the capability for integrating risk analysis into the event analysis process; and
- Feed forward key results to facilitate enhancements in and support of the various NERC programs and initiatives (e.g., performance metrics, standards, compliance monitoring and enforcement, training and education, etc.)[26]

While the full or partial loss of a single EMS or SCADA system may not result in the blackout depicted in the task force scenario, analysis of the causes of such a loss could be helpful in correcting conditions on the utility's EMS or SCADA system and possibly lead to the identification of useful lessons learned for the industry. However, in the case of a coordinated

[26] NERC Event Analysis Program

attack, impacting potentially multiple EMS and SCADA systems, it is imperative to capture the relevant actions and responses across each utility to create an accurate timeline similar to the 2003 Blackout.

Details of intrusions or compromises should also be incorporated into attack trees to continue to build on the catalogue of attack vectors and vulnerabilities.

Procurement Language

A significant amount of work has been done by DOE, DHS, the national labs and electricity industry to create contractual language that entities can use when acquiring systems and equipment from vendors. EMS, SCADA and field devices often have a much longer operational lifetime then traditional IT business systems. By obligating vendors to provide documentation and evidence of security features, entities are better equipped to do adequate acceptance testing as well as properly design defensive measures when built-in security features need to be augmented.

See reference section for a link to the Cyber Security Procurement Language for Control Systems.

Independent Testing of Systems and Equipment

Identifying and alerting the electricity sector of vulnerabilities so mitigation steps can be implemented is an important way to limit the number of successful attack vectors. Establishing partnerships between independent testing groups, hardware and software vendors and ICS-CERT and ES-ISAC encourages vulnerabilities to be identified and industry alerts issued in concert.

Unfortunately, the independent testing community is not always in synch with the hardware and software community when it comes to prioritizing the threats or even agreeing that there is a vulnerability. Recent examples involve the S4 Project Basecamp initiative where six ICS devices were evaluated, vulnerabilities identified, and exploit code made publically available. This partnership needs further development so the time between discovery of the vulnerability, disclosure of exploit code and release of patches or alerts is minimized as much as possible.

Responses to Attack

Background

Since the 2003 Blackout Report, the electricity sector has stressed the importance for system operators to maintain situational awareness of their respective systems. In the case of Reliability Coordinators (RC) there is also the need for these RC's to maintain situational awareness over a wide area (an area the extends beyond the operating zone of the RC). To achieve situational awareness the electricity sector has over the past decades developed increasingly sophisticated network applications, meters, and telemetry to paint the view of the system in ever more accurate terms. Often times these systems refresh for the operators every few minutes and in some case every few seconds.

Cyber Security experts often stress the importance of being able to protect the confidentiality and integrity of data and information, and the availability of systems/applications. While the confidentiality of our customers and member's data is very important a breach of this pillar of security does not necessarily jeopardize system reliability.

In spite of these applications having availability rates in the 99% range, these systems do occasionally fail. As such, every operating entity has back-up, call-out, and response plans to rapidly diagnose and address the rare application crashes.

Just as important as the system operations applications is the data and communication paths that feed these applications. These applications typically pull in thousands of data points from transmission sub-stations, lines, and generators every few seconds. In addition, entities are dependent on understanding and reacting to systems conditions with their neighbor's assets as well.

Cyber Security experts often stress the importance of being able to protect the confidentiality and integrity of data and information, and the availability of systems/applications. While the confidentiality of our customers and member's data is very important a breach of this pillar of security does not necessarily jeopardize system reliability.

In contrast the impacts associated with attacks on integrity (are outputs trusted?) and availability (are outputs meaningful and timely?) can have profound impacts on reliability.

The ideal response for these systems when under attack is to gracefully degrade in terms of capability without a material effect on operational reliability. This might mean, for example, that non-essential tools and functionality are shed, but control and communication with generating plants is maintained. If not already in place, this would require clear separation between core system reliability functionalities and business and market systems, external networks, and non-essential inputs. Networks should be designed such that these services can be quickly and easily disconnected from critical reliability functions at a moment's notice

without affecting operational reliability. This will essentially allow system operators to "fly with fewer controls."[27]

Identification of those core systems and functions that are essential to maintaining operational reliability would include:

- EMS (energy management system) – a control system with a suite of applications that provides decision support capability to monitoring and controlling the transmission system.
    - "Model" the heart of the EMS which replicates the portion of the grid the entity is responsible for operating,
    - State Estimation (SE) the way in which the model/EMS can estimate points not physically monitored (i.e. calculate the readings in the middle of a line with data from the readings on both ends of the line) and,
    - Security Analysis (SA) the more advanced applications of the EMS that conduct the "What If" contingency analysis so that operators can always position the system in a conservative/reliable state.
- GMS (generation management system) – the suite of applications that enable an entity to keep generation and other resources in balance with load.
- Ability to maintain communications control centers and field equipment (i.e. RTUs) to provide input to EMS/GMS.
- Core skilled workforce availability.

Isolation and Survivability

Survivability involves focusing on protecting those systems and functions that are essential to maintaining reliable operations. Reliable operations will degrade, over time, resulting in the gradual reduction in services and functions until essential operations are no longer possible. The key is trying to maintain reliable operations in a reduced state for as long as possible. This resilience characteristic is known as graceful degradation of service.

A number of survivability and isolation tactics are outlined in Appendix G.

There are difficulties associated with isolation. Monitoring and situational awareness suffers as automated processes designed to inform operational staff are systemically severed. This includes both internal monitoring as well as connectivity with neighboring utilities. Bulk Power System control centers can pose risks to other BPS control systems via essential communication links. Internal data corruption, man in the middle scenarios, malicious code injections are all possible scenarios that must be considered when evaluating the operational impact that one control system may have on other externally connected control systems. Physically deploying

[27] High-Impact Low-Frequency Event Risk to the North American Bulk Power System page 37

staff to locations to determine status and relay information to operators in control centers would be challenging for an extended period of time.

Once integrity has been verified on end devices and communication paths, connectivity can be re-established. However, monitoring should be continued to ensure a re-occurrence of the disruption does not happen nor develop without operator recognition.

Restoration

Restoration from a coordinated cyber attack could introduce conditions that are not normally encountered during restoration from hurricanes or other types of probabilistic events.

Restoration from a coordinated cyber attack could introduce conditions that are not normally encountered during restoration from hurricanes or other types of probabilistic events

During a cyber attack and the following aftermath, responders may be lulled into the false sense of security that there is only one wave of assault. As with a storm, once the storm passes, everyone pitches in to begin the restoration process with a clear and understood recovery plan. If the attack vector(s) and techniques/tools for the attack are not fully understood and mitigated, the attacker could launch subsequent attacks to disrupt recovery efforts or respond to mitigation efforts. These later attack waves may hold devastating impact potential if not understood and expected.

To ensure the attack vector(s) and methods have curtailed and can't be restarted, entities may need to restore application files and operating systems to a safe or trusted release. This can introduce problems or delay recovery due to any entity installed modifications. In addition, certain types of attacks can render hardware or other equipment inoperable. Consequently, new equipment may have to be acquired and installed. Manufacturer assistance may need to be obtained.

Restoration of situational awareness may have to be manually implemented with staff physically stationed at key locations until communication with monitoring equipment and associated telemetry is restored. Restoration may also involve repair or replacement of parts suffering physical damage from a cyber event. Some of these may require long lead times for replacement due to supply chain or skilled installation workforce availability issues.

Safety plays an even more important role during recovery than before. Because systems and equipment may behave unpredictably during restoration, extra caution should be communicated to staff to make them aware of this issue.

Forensics

Determining the actual cause of an attack is difficult at best even with logs and other monitoring and intrusion detection capabilities found on business system networks. On the operational side of the Bulk Power System, equipment and software are not always capable of capturing information necessary to do a proper forensic analysis. Nonstandard protocols,

legacy architectures that can be several decades old, and irregular or extinct proprietary technologies can all combine to make the creation and operation of a cyber forensics program challenging.[28]

To aid asset owners and operators in this preparation, ICS–CERT has identified key elements for developing incident response capabilities necessary to collect data and perform follow-on actions to restore systems to normal operation.

One of the key elements is preserving forensic data. This includes methods for collecting, analyzing, and reporting these data, all of which are important components of any plan to avoid loss of essential information, provide for rapid operational restoration, and improve both near and long-term mitigation and security strategies. The following activities are recommended for preserving these important data in the event of a suspected incident.

- Keep detailed notes of what is observed, including dates/times, mitigation steps taken/ not taken, strange or unusual operational behavior, device logging enabled/disabled, and machine names for suspected compromised equipment. More information is generally better than less information.
- When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a machine suspected of being compromised from the network.
- Capture forensic images of the system memory and hard drive prior to powering down the system.
- Avoid running any antivirus software "after the fact" as the antivirus scan changes critical file dates, which impedes discovery and analysis of suspected malicious files and timelines.
- Avoid making any changes to the operating system or hardware, including updates and patches, because they will overwrite important information about the suspected malware.[29]

The ICS-CERT provides onsite incident response, free of charge, to organizations that require immediate investigation and resolve in responding to a cyber attack. Upon notification of a cyber incident, ICS-CERT will perform a preliminary diagnosis to determine the extent of the compromise. At the customer's request, ICS-CERT can deploy a fly-away team to meet with the affected organization to review network topology, identify infected systems, image drives for analysis, and collect other data as needed to perform thorough follow-on analysis. ICS-CERT is able to provide mitigation strategies and assist asset owners/operators in restoring service and provide recommendations for improving overall network and control systems security.[30] ICS-CERT cannot, however, conduct criminal investigations.

[28] Recommended Practice: Creating Cyber Forensics Plans for Control Systems

[29] ICS-CERT Monthly Monitor July/August 2011

[30] DHS – Industrial Control System Computer Emergency Response Team (http://www.us-cert.gov/control_systems/ics-cert/more_information.html)

Entities that utilize outside services to assist with forensics or possible criminal prosecution should make sure the service provider or law enforcement agency is aware of all operational requirements and obligations. This could preclude on inhibit the collection of certain evidence (i.e. hardware and software) as part of the investigation.

See reference section for links to documents related to establishing a forensics program for control systems.

If prevention eventually fails, preparedness to detect the compromise before impact is realized is the next goal. The same data sources that lead to a sound post-incident forensics analysis will also provide the mechanisms to proactively detect and deter successful compromises.

These data sources include standard IT infrastructure logging such as firewall and intrusion detection systems. Secondary data sources that have proven to be invaluable during detection and forensics include Netflow data, Domain Name Resolution (DNS) logging, proxy logging, Email (SMTP) Logging, Remote Access (VPN) logging and full packet captures. It is recommended to extend the retention of these logs as long as feasible to maintain the historical forensics capability.

Once the above data sources are logged, they may be correlated together to give context of the source of the intrusion and the methods the adversary may be using. This correlation of key artifacts may be distilled into what is known as Indicators of Compromise (IOCs) which can allow for detection for follow-on attempts or sharing with the industry through trusted partners such as the ES-ISAC or ICS-CERT.

Recommendations

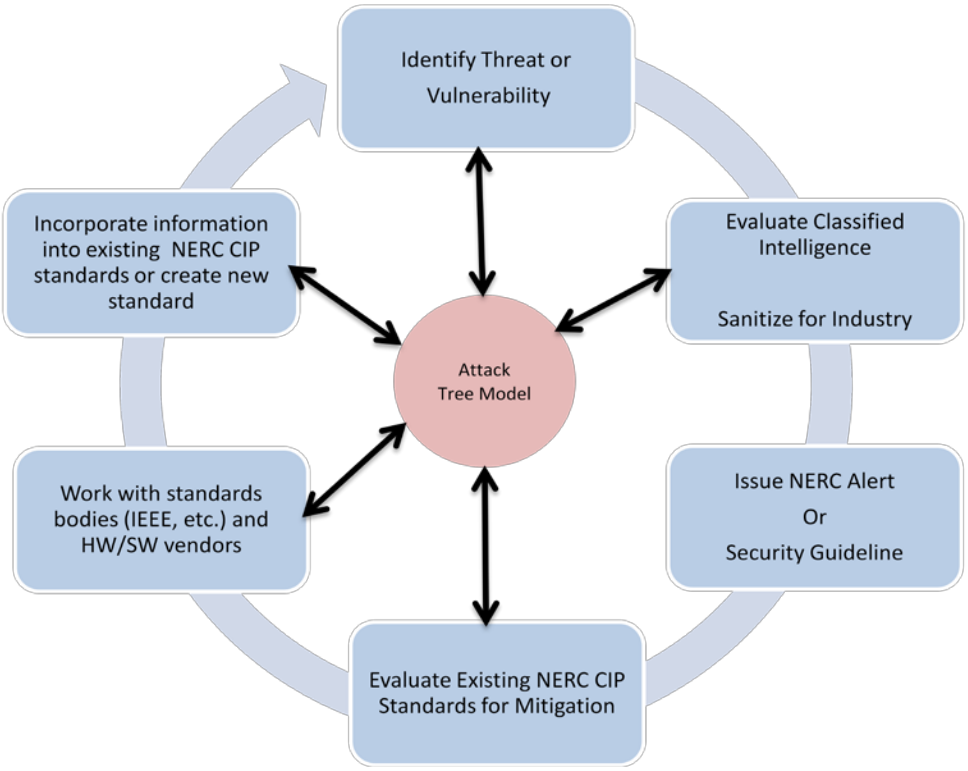
Following are the recommendations from the task force:

- **Continue to build on the Attack Trees -** A significant amount of work has gone into creating the attack tree framework, however recommendations from detailed analysis have not been completed. The top level root node of the attack tree is very specific to the task force scope, but lower level branches are applicable to many other scenarios such as attacks on generation, transmission/distribution or disrupting situational awareness.

  A separate working group under NERC's Critical Infrastructure Protection Committee (CIPC) should be established to further develop attack trees with the goal of populating the nodes, performing detailed analysis and providing recommendations to industry from this analysis.

  While these trees will never be finished, they do provide a solid structure to build on. For example, for each revision to the CIP standards the new requirements could be incorporated into the attack trees and analysis rerun to determine any positive or negative consequences of the propose changes. Prior to release of a NERC Alert, compare mitigation measure actions against the attack trees to determine if the recommendations provide the greatest likelihood of reducing the potential for compromise. At least annually evaluate the attack trees to incorporate new information.

  Because of the sensitive information captured and developed, the attack trees should be stored and managed as part of the NERC ES-ISAC documentation library, or in some cases, on classified systems.



- **Continue to develop security and operations staff skills to address increasingly sophisticated cyber threats -** Utilities should seek or develop methods to rapidly build the cybersecurity skills needed to enhance the security and reliability of the nation's electricity delivery system. Training programs should create development plans based on job roles and identified competencies to ensure that content and delivery addresses both knowledge and skill building. Hands-on development trainers are needed to provide practice opportunities and customize training. Aptitude assessments should be used to help tailor development efforts to meet the needs of individuals and teams and assess development effort effectiveness.

  Development efforts should include challenging cyber attack scenarios that are customized to the utility's technology environments and business operations. Development efforts should recognize gaps in the knowledge, skills, and abilities of cybersecurity personnel in detecting and responding to these threats.

  Entities should maintain an understanding of the current cyber threat as it applies to the electric sector; develop the skills to maintain situational awareness of that threat; strengthen the capability to match the external threat environment to the internal environment; and develop staff capability to use threat intelligence to best protect their organizations.

  Development programs should identify the skill components most in need by both security and operations job roles, and use assessment tools that will ensure that the programs produce the right skills and knowledge. These efforts should be applied beyond traditional information security environments and include the SCADA emergency management system, automated generation control, plant-level control systems, protection/safety systems, and field equipment.

- **Augment Operator Training with Cyber Attack Scenarios** – Several cyber attack scenario templates are included in Appendix C of this report. Existing Operator Training Simulators (OTS) or Dispatcher Training Simulators (DTS) should be leveraged to include cyber attacks. If these scenarios can be realistically captured and simulated, operators and technical staff could train under realistic conditions to recognize, react, respond, and defend against cyber-attacks before they ever encounter one in a production setting. The training should include collaboration and teamwork with physical and cyber security experts.

- **Conservative Operations -** Conservative Operations is an operational state resulting from the intentional actions taken in response to unknown, insecure, or potentially risky system conditions in order to move to a known, secure, and low-risk operating posture.

  A significant amount of work in preparing for conservative operations is documented in the Severe Impact Resilience: Considerations and Recommendations report created by the Sever Impact Resiliency Task Force. Entities should review this document for applicable best practices.

- **Continue to endorse existing NERC initiatives that help entities prepare for and respond to a cyber attack –** NERC has a number of initiatives that can help the industry with cyber attack identification, defense and response. Three examples are:
    - Cyber Readiness Preparedness Assessments (CRPA)
    - NERC Grid Security Exercise
    - ES-ISAC portal and collaboration

  The 2010 CRPA report identified eight observations and associated recommendations that came from 10 utility assessments. Each company should review the recommendations outlined in Appendix I for applicability to their program.

  Over 70 entities participated in the first NERC Grid Security Exercise. This provided an opportunity to test both internal and industry responses and communication capabilities.

  The CIPC should encourage entities to participate in all three efforts to fine tune their response plans. NERC should continue to fund and provide the necessary resources to expand the number entities that can participate in these programs.

- **Conduct exercise with Transmission Planners –** The bulk power system is inherently highly resilient to threats. Probabilistic planning criteria consider a wide range of potential contingencies and consider probabilistic failure (i.e. equipment failure, human error, and weather events) yet do not consider a structured, coordinated, and intelligent attacker. Additionally, the definition of a "single asset" under this criterion is often based on the probabilistic failure of a given system component (i.e. a single bus or circuit breaker or a single unit at a generating plant) and may not cover the loss of every component at multiple given physical locations (i.e. several entire substations or generating plants), as could be effected by a physical attack. Cyber attacks take this one step further by creating the possibility that an asset could be misused to affect assets connected to it. Consider the example of a large substation with multiple generating units connected to it. Though this capability has not been successfully demonstrated to date, an experienced cyber attacker could use relays and breakers within that substation to affect the operation of each of those plants.

  In order to accurately evaluate the system's resilience to structured attacks, the sector should work to incorporate these new perspectives and take a broader view of the system than is generally provided by traditional system planning and operating criteria. Entities within the sector have conducted such analyses with results that indicate the system would retain its integrity in the event of certain targeted attacks, however this practice should be considered more widely as planning methods evolve. Priority should be given to designing for survivability, such that the system could withstand and recover from a structured multi-

node attack. At a minimum, system planners and operators should be able to model the effects of such an attack and drill restoration measures.[31]

Working with Department of Energy national labs and a pilot group of electricity utilities, a transmission planning exercise should be coordinated by NERC to simulate a coordinated cyber attack that creates a cascading event and blackout. The event should attempt to identify the point at which current transmission planning criteria is exceeded and how to deal with dynamic mitigation. The results could provide insight into additional facilities/locations that might need protection beyond what is called for with the CIP and Transmission Planning (TPL) standards.

The exercise scenarios should be selected from a comprehensive hazard analysis method, such as using the attack tree work completed by the CATF or selecting another rigorous approach to identify and bound the attack scenarios.

- **Increase Awareness for Department of Energy Initiatives -** The Energy Sector Control Systems Working Group recently released the latest Roadmap to Achieve Energy Delivery System Cybersecurity. There are numerous initiatives that will help ensure protection of critical systems supporting the Bulk Power System going forward. In addition, the document serves as an excellent reference document that all entities can benefit from reading. Two initiatives that can have an immediate benefit are:

    - **Digital Bond / DOE – Bandolier initiative:** Digital Bond's Bandolier project helps asset owners and vendors identify and audit optimal security configuration for industrial control system (ICS) servers and workstations. Digital Bond partners with leading ICS vendors to identify the optimal security configuration that still allows the vendor's product to operate properly. This requires access to the vendor's security experts, lead engineers and a test lab. Digital Bond then creates Bandolier Security Audit Files that work with the compliance plugin in the Nessus vulnerability scanner. Bandolier Security Audit Files are available for over twenty control system components, with more on the way.

      http://www.digitalbond.com/tools/bandolier/

    - **Digital Bond / DOE – Portaledge Project:** Portaledge is a Digital Bond research project that **aggregates** security events from a variety of data sources on the control system network and then correlates the security events to identify cyber attacks. Portaledge leverages the aggregation and correlation capability of OSIsoft's PI server, and its large installed base in the energy sector to provide this cyber detection capability in a system many industrial control system (ICS) owner / operators already have deployed.

      http://www.digitalbond.com/tools/portaledge/

[31] High-Impact Low Frequency Event Risk to the North American Bulk Power System page 36

- **Continue to Extend Public / Private Partnership** – More and more US and Canadian electricity sector staff have been granted clearances to see classified information. As the US and Canadian Intelligence Communities working with NERC discovers new vulnerabilities and threats, this information should be disseminated to the electricity sector as quickly as possible. The electricity industry must ensure an appropriate mix of operational, security, technical and managerial staff is cleared and available to evaluate, respond and make timely decisions to slow or stop an attack.

  Effective information sharing can be enabled in multiple ways including having clearances passed to local FBI offices and Fusion Centers so expedited secure communications can be accomplished with a wider portion of the industry. It is important to ensure the inclusion of the appropriate representation from the law enforcement community, as the traditional separation of tactical field operations and national security operations do not necessarily facilitate the proper sharing of information. In Canada, jurisdiction for Canadian electricity utilities varies from province to province. The provincial law enforcement agencies have a reporting relationship with the Royal Canadian Mounted Police (RCMP).

  In addition, NERC and federal agencies should continue to involve sector experts to help translate classified information (e.g. preparing useful tear-line material) into alerts that can be issued to the industry. This re-enforces the life cycle approach to addressing vulnerabilities.

  The ES-ISAC offers an increasingly robust portal environment to organize electronic collaboration and this development effort should be strongly supported. ES-ISAC is establishing protective procedures to provide insulation from compliance concerns which might otherwise limit the willingness to share vital security information before, during or after a contingency. In the event standard information sharing protocols are unavailable during an attack (e.g. between utilities, ES-ISAC, etc), alternative methods need to be defined.

  In parallel, the electricity sector needs to improve its sharing of information with federal agencies. Historically, there has been and continues to be a reluctance to do this because of the uncertainty about where the information could end up or that the disclosure could result in a perceived compliance violation.

Outreach

Outreach is an important part of asserting deliberate intent of the sector to cause transformative change. If the goal is to fortify sector security against a coordinated cyber attack, outreach activity will raise awareness of the issue and equip sector participants with the motivation and knowledge to enhance capabilities.

SUCCESS ELEMENTS	WHAT IT MEANS…	ACTIONS
Skilled Workforce	Long-term workforce development providing scale and capacity of vital skill sets and qualifications in security related professions and trades.	• Work in conjunction with National Board of Information Security Examiners (NBISE) initiatives to enhance workforce development in both IT and OT security • Encourage continued participation in Advanced Industrial Control System Red/Blue Team Training offered by Idaho National Labs.
Leadership Engagement	Leaders driven by passionate focus on security viewed as a strategic competitive advantage at entity, sector, national and international levels.	• Provide periodic updates to the NERC CIPC, ESCC on status of Cyber Attack Task Force and any follow-up working group activities.
Vertical Communications	Effective two-way communications between authoritative information sources and entities.	• Report events to the ES-ISAC, the FBI and applicable Canadian law enforcement agencies to better identify trends • Engage FBI, DHS and DOE resources to provide input to attack trees • Coordinate with DOE, the national labs and DHS on other cyber attack programs, both at the classified and unclassified level. • Communicate with FERC and Congressional staff (through NERC and Industry Trade Associations) to educate regulators about the work being done by the electricity sector.
Horizontal Communications	Communications between proactively engaged entities sharing issues, opportunities, perceived gaps and best practices.	• Encourage entity sharing of information with ES-ISAC related to systems events. • Participate in initiatives such as those offered by NESCO

Communications Content	Comprehensive with holistic integration of threat, vulnerability, planning, operational, mitigation, and process issues. Standard lexicon, formats and redundant, interoperable, classification controlled pathways are employed.	• CIPC members and other Subject Matter Experts should continue to work closely with the NERC ES-ISAC on timely and relevant alerts
Advanced Technology Application	Provision and use of cost effective, sustainable technologies and services. Vendors and supply chain participants are energized and innovative --committed to trusted secure supply chains and optimal new product development, informed by sector expertise, emerging threats and real vulnerability gaps.	• Work with the Energy Sector Control Systems Working Group on enhancements and updates to the Roadmap to Achieve Energy Delivery Systems Cybersecurity

References

Name	Link
DOE/NERC HILF "*High Impact, Low Frequency Risk to the North American Bulk Power System*" report	http://www.nerc.com/files/HILF.pdf
Critical Infrastructure Strategic Roadmap	http://www.nerc.com/docs/escc/ESCC_Strat_Roadmap_V5_20_Oct2010_clean.pdf
NERC Technical Committees' Report – *Critical Infrastructure Strategic Initiatives Coordinated Action Plan*	http://www.nerc.com/docs/ciscap/Critical_Infrastructure_Strategic_Initiatives_Coordinated_Action_Plan_102510.pdf
NERC Scope: Cyber Attack Task Force	http://www.nerc.com/filez/catf.html
Roadmap to Achieve Energy Delivery Systems Cybersecurity – September 2011	http://www.controlsystemsroadmap.net/pdfs/roadmap.pdf
NERC CIP Standards	http://www.nerc.com/page.php?cid=2|20
Insider Threats to Utilities	DHS Office of Intelligence and Analysis – July 19, 2011 Note
US Electricity Sector Faces High Cyber Exploitation Threat, Low Cyber Attack Threat	FBI presentation, http://www.nerc.com/docs/cip/CIPC%20Presentations%20September%202011.zip
NERC Cyber Risk Preparedness Assessment – Tabletop Exercise Report April 2010	http://www.esisac.com/Public%20Library/Reports/CRPA%202010%20Report.pdf
DHS Report – Preventing and Defending Against Cyber Attacks – June 2011	http://www.dhs.gov/xlibrary/assets/preventing-and-defending-against-cyber-attacks.pdf
DHS Recommended Practice: Creating Cyber Forensics Plans for Control Systems	http://www.us-cert.gov/control_systems/pdf/Forensics_RP.pdf
DHS Cyber Threat Source Descriptions	http://www.us-cert.gov/control_systems/csthreats.html
Recommended Practice: Creating Cyber Forensics Plans for Control Systems	http://www.inl.gov/technicalpublications/Documents/4113665.pdf
DHS -	http://www.us-cert.gov/control_systems/pdf/Incident_Handling_Brochure_Nov_2010.pdf

The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems	http://www.tofinosecurity.com/professional/use-attack-trees-assessing-vulnerabilities-scada-system
Developing an Industrial Control Systems Cybersecurity Incident Response Capability, 2009	http://www.usert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf.
NIST SP800-86 Guide to Integrating Forensic Techniques into Incident Response	http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
NIST 800-61, "Computer Security Incident Handling Guide	http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
National Electric Sector Cyber Security Organization	http://www.energysec.org/nesco
Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies	http://www.us-cert.gov/controlsystems/practices/RecommendedPractices.html
ERO Event Analysis Process	http://www.nerc.com/filez/eawg.html
NSA Manageable Network Plan	http://www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlan.pdf
DHS Procurement Language for Control Systems	http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf
National Response Framework	http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf
SANS 20 Critical Security Controls	http://www.sans.org/critical-security-controls/

NERC CATF Roster - Contributors

Last Name	First Name	Company
Abell	Charles	Ameren (Vice Chair)
Allen	Ron	AEP
Assante	Michael	NBISE
Baumken	David	Public Safety, Canada
Berrett	Dan	DHS
Bowe	Tom	PJM
Brindley	Stuart	NERC
Diebold	Stephen	KCP&L
Dunfee	Rhonda	DOE
Eng	Carl	Dominion
Engels	Mark	Dominion (Chair)
Fabro	Mark	Lofty Perch
Goff	Ed	Progress Energy
Gray	Jeff	DHS
Hintermister	Fred	NERC
Ingoldsby	Terry	Amenaza
Johnson	Michael	APX Power Markets
Kulseth	Christopher	MRO
Le	Bao	Coalfire Systems
Lemay	Francois	Hydro-Quebec
Miller	Ben	NERC
Morgan	Jeff	FBI
Roberts	Don	Southern
Roxey	Tim	NERC
Ryan	Kelly	NERC
Whitney	Tobias	GE Energy

NERC CATF Roster - Observers

Last Name	First Name	Company
Anderson	Jeff	Open Access Technology International
Anne	Pramod	NextEra / FPL
Bacik	Sandy	Enernex
Batz	Dave	EEI
Braendle	Markus	ABB
Brake	Lloyd	DOD
Brain	Steve	Dominion

Last Name	First Name	Company
Breed	Ryan	ERCOT
Bugh	Larry	RFC
Calder	John	Dominion
Ciliberti	Carlo	Lockheed Martin
Crabtree	Jeff	MRO
Dakin	Rick	Coalfire Systems
Dodd	Gary	Bonneville Power Administration
Eigenhuis	Scott	Puget Sound Energy
Falkovich	Mikhail	PSEG
Farmer	Randy	Lockheed Martin
Flowers	Tom	EPRI
Frank	Daniel	Sutherland
Freese	Jerry	AEP
Fuller	Jeffrey	Dayton Power & Light
Gaudette	Marc	Dominion
Goodrich	Greg	NYISO
Gordon	Bill	AEP
Harriman	Bob	BC Hydro
Haskins	Linda	Dominion
Kemp	Karen	Direct Energy
Keoseyan	Scott	Deloitte and Touche
King	Morgan	WECC
Kingbaum	Forrest	Bonneville Power Administration
Lackey	Kevin	ERCOT
LaVoy	Lanse	DTE Energy, Inc.
Lim	John	Consolidated Edison
Loftis	John	Dominion
McGlynn	John	PJM
Parcel	Sean	AEP
Raesis	George	Entergy
Rosenstiel	Richard	Exelon
Shah	Ashish	Deloitte and Touche
Stockton	Paul	DOD
Tibbs	Clark	Vertical Horizons
Webber	Laurent	Western Area Power Administration
Wells	Rita	INL
Weiss	Joe	Applied Control Solutions
Whitney	William	Garland Power & Light / City of Garland
Williams	Ramsey	PG&E
Willson	James	DOD
Woodzell	Matt	Dominion

Appendix A: Introduction to Attack Trees

Threat trees are the first component of an attack tree. Threat (or fault) trees are used to determine whether the conditions necessary for a threat to be realized exist and are un-mitigated. A threat tree consists of threat outcomes:

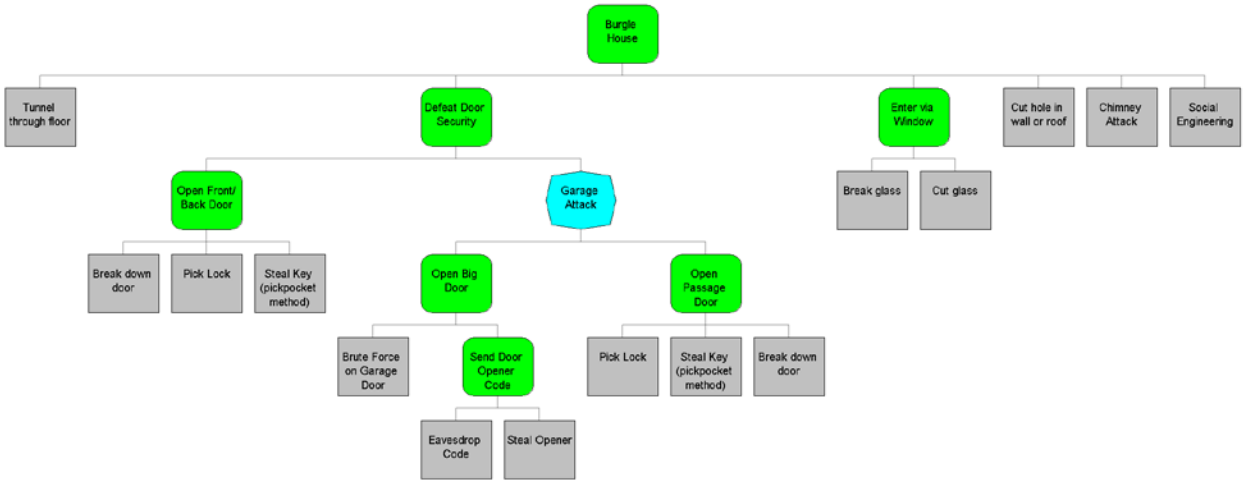
(e.g., long-term service disruption to a large area), in which preexisting conditions that must be true for an adversary to realize the threat (e.g., a circuit breaker is accessible through Internet connectivity). Any condition can, in turn, have one or more preconditions. Two or more conditions at the same level and sharing the same parent node can be combined, resulting in an "and" relationship; otherwise, an implicit "or" condition exists. Determining whether one or more vulnerabilities are associated with a threat is simply a matter of starting at a leaf condition (a node in the threat tree with no child nodes) and following it up to the root threat. If a path is unbroken by a mitigated node or a broken "and" condition exist, a vulnerability exists.

This information combined with intelligence about adversaries can be used to create an attack tree. Certain vulnerabilities are more likely to be exploited based on the attacker's capabilities (resources, geographic location, and industry experience.), while others will be virtually impossible to exploit.

The impact of a threat can be calculated quickly from the attack tree, which can, in turn, be used to justify or inform expenditures or resource allocation planning on mitigation strategies. Impact can be calculated by adding the financial and operational impact of the root of the tree to any impact created as attackers work their way up the tree. Some of the intermediate nodes in the tree may have an adverse impact, even if the attacker doesn't have the capabilities to extend further up the tree.

Once an impact is calculated, it is possible to calculate the value of investing in mitigation strategies. Based on the impact and the likelihood of occurrence, it is possible to determine whether countermeasures should be used for that vulnerability – or whether the vulnerability is so difficult to exploit (or has so little impact) that countermeasures are unnecessary.[32]

[32] American Electric and Power Attack Tree Methodology


Burgle House
Tunnel through floor
Defeat Door Security
Enter via Window
Cut hole in wall or roof
Chimney Attack
Social Engineering
Open Front/ Back Door
Garage Attack
Break glass
Cut glass
Break down door
Pick Lock
Steal Key (pickpocket method)
Open Big Door
Open Passage Door
Brute Force on Garage Door
Send Door Opener Code
Pick Lock
Steal Key (pickpocket method)
Break down door
Eavesdrop Code
Steal Opener

Appendix B: Resources

United States

- NERC Electricity Sector – Information Sharing and Analysis Center (ES-ISAC)
  http://www.esisac.net/SitePages/Home.aspx
- Department of Homeland Security
  - United States Computer Emergency Response Team (US-CERT)
    http://www.uscert.gov/
  - Industrial Control System – Computer Emergency Response Team (ICS-CERT)
    http://www.uscert.gov/control_systems/ics-cert/
  - Control Systems Security Program
    http://www.us-cert.gov/control_systems/cstraining.html#workshop
- International Computer Emergency Response Teams
  http://www.internationalcybercenter.org/certicc/certworld
- National Council of Information Sharing and Analysis Centers (ISACs)
  http://www.isaccouncil.org/index.php?option=com_content&view=article&id=87&Itemid=194
- Federal Bureau of Investigation
  http://www.fbi.gov
  http://www.infragard.net/
- Domestic Security Alliance Council

  http://www.dsac.gov/Pages/index.aspx

United Kingdom

- CPNI – Center for the Protection of National Infrastructure

http://www.cpni.gov.uk/

- SOCA – Serious Organized Crime Agency

http://www.soca.gov.uk/

Canada

- RCMP – Royal Canadian Mounted Police

http://www.rcmp-grc.gc.ca/index-eng.htm

- CCIRC – Canadian Cyber Incident Response Center

http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

New Zealand

- CCIP – Center for Critical Infrastructure Protection

http://www.ncsc.govt.nz/

Australia

- AFP – Australian Federal Police

http://www.afp.gov.au/

- CERT Australia – Computer Emergency Response Team

http://www.auscert.org.au/

Vendor Alerts

- ABB – www.abb.com
- Alstom Grid – www.alstom.com/grid/products-and-services/electrical-network-systems/
- Open Systems International – www.osii.com
- Schweitzer Engineering Laboratories – www.selinc.com
- Siemens – www.seimens.com

Appendix C: Cyber Event Scenarios for System Operators

Overview

The following scenarios are presented in order from more plausible to less plausible. Plausibility is based on the perceived ease with which a malicious individual could accomplish the task. The scenarios are centered on operator trainee actions as opposed to support personnel actions.

We identified at least four major categories of events, and chose scenarios from among these:

- Social engineering
- Denial of service
- Spurious device operation
- Realistic data injection

Almost all of the symptoms described in these scenarios could, and in overwhelming likelihood would arise from any number of problems *other* than a cyber attack. These other likelihoods should be considered before a cyber attack is assumed.

Social Engineering – false request or information to operator

Description

In this scenario, a malicious individual contacts an operator and makes a request for action or information, or supplies false information. This individual could be a disgruntled current or former employee. They could represent themselves as field personnel, and RTO employee, or any number of legitimate individuals.

Implementation

During a training exercise a phone call could be made to the trainee, with the individual asking for an action or supplying false information.

Example: “Hello, this is John Doe at Metropolis substation. We’ve got a big problem here and need you to open the 1A breaker ASAP.”

Recognition

Awareness and a questioning attitude are probably the best tools for recognizing this scenario.

- Is this an unusual request?
- Is this a familiar identifiable person?
- Does this person possess particular knowledge about the situation when asked?
- Is this one of many unusual or suspicious requests?

Response

If a suspicious request is received, obviously the trainee would not act on it. They should:

- Try to gain more information from the caller if possible
- Consider the appropriateness of the request
- Attempt to identify the individual
- Verify the request with another entity (cross check)
- If the situation remains suspicious, report the incident to their appropriate supervision and support personnel

Denial of Service – EMS network

Description

EMS computer network becomes fully or partially unavailable, or network performance declines. Scenario proposes that malicious activity has adversely affected EMS network.

Implementation

This is most easily staged in a training simulator environment, or even on a separate training network. Any number of methods could produce the appearance of network loss or overload.

- Disconnect operator workstations from network at a location unseen by the trainees
- Remotely alter workstation or training network settings such that slow network response is observed
- Administratively terminating workstation sessions may give the appearance of network loss

Recognition

- EMS system may seem completely unresponsive
- User interface may spuriously disconnect then reconnect
- May experience timeouts when performing actions
- May experience multiple telemetry failures
- Other evidence of unauthorized system access exists or was suspected

Response

- Consider the extent of symptoms – one or two workstations, entire system, other corporate non-EMS systems
- Contact I.T. support staff
- Consider a move to offsite disaster facility while support staff secures primary EMS facility

Denial of Service – EMS applications halted

Description

Certain applications on the EMS have been maliciously halted. Therefore, the EMS system is not providing proper updates. Could be coupled with control compromise or physical sabotage in the field – the trainee of course would not be aware of it.

Implementation

Most likely requires a training simulator environment. In that environment, key applications such as the alarm system or data scanning applications are quietly halted. This might be accompanied by simulated manipulation of the actual power system while these programs are unavailable.

If the situation should go unnoticed, a simulated call from field personnel asking about a particular situation might call attention to the lack of updates.

Recognition

- EMS system does not appear to be updating
- May be lack of EMS alarms for an extended period
- Phone call from other personnel reporting changes not reflected in EMS
- When EMS system is restored, a large number of changes might be indicated
- Other evidence of unauthorized system access exists or was suspected

Response

- Cross check indicated data with other personnel or systems
- Notify support staff

Spurious Device Operations

Description

Multiple, un-commanded, unexpected device operations indicated in EMS system. Scenario could be based on:

- Indication-only compromise (devices aren't actually changing)
- Control compromise (devices are actually being manipulated)

Implementation

Most likely requires a training simulator environment. In that environment, event scenarios could be devised to:

- Simulate compromised telemetry, such that false indications and alarms are present
- Alter the power system simulation, such that power system devices actually operate (simulate a control compromise)

Recognition

- Unexpected state changes
- Could be multiple changes at unrelated locations
- May be conflicting indications (e.g. breakers open but flow present)
- Other evidence of unauthorized system access exists or was suspected
- State estimator may indicate that data is conflicting

Response

- If possible verify indications (cross-check)
- Verify with field personnel
- Call support staff

Realistic Data Injection

Description

Convincing injection of false data into EMS or associated systems, for the purpose of changing operator behavior. This is much more subtle than strict denial of service and requires much greater knowledge of the system. Examples of changed operator behavior:

- Convince them to shed load
- Convince them to allow equipment overload/damage
- Cause then to ignore changes taking place on the power system

Implementation

Most likely requires a training simulator environment. In that environment, event scenarios could be devised to bias operator indications so that they do not match the true power system simulation. The power system simulation may be trending toward an adverse state, and this would be unknown to the trainee.

Recognition

The fact that this attack is very difficult to accomplish completely can help in recognition. It is possible the offender would make mistakes such that some indications would not look normal.

- Lack of correlation between measurements
- Indications defy known system conditions
- Some indications appear abnormal (offender failed to accomplish convincing injection)
- State estimator may flag anomalies where they didn't previously exist
- Other evidence of unauthorized system access exists or was suspected

Response

- If possible verify indications (cross-check)
- Verify with field personnel
- Call support staff

Appendix D: Acronyms

AGC	Automatic Generator Control
BA	Balancing Authority
CA	Critical Asset
CCA	Critical Cyber Asset
CIPAC	Critical Infrastructure Partnership Advisory Council
CIPIS	Critical Infrastructure Protection Information System
CIPC	Critical Infrastructure Protection Committee
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
DOS	Denial of Service
DDOS	Distributed Denial of Service
EGSEC	Energy Grid Security Executive Council
EMS	Energy Management System
ES3P	Electricity Sector Public Private Partnership
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
ESP	Electronic Security Perimeter
ESCC	Electricty Sub-sector Coordinating Council
ICCP	Inter- Control Center Communication Protocol

ICS	Industrial Control System
IDS	Intrusion Detection System
IP	Internet Protocol (see TCP/IP)
IPS	Intrusion Prevention System
MAC	Media Access Control
MD5	Message Digest 5
OS	Operating System
PLC	Programmable Logic Controller
POTS	Plain Old Telephone Service
RC	Reliability Coordinator
RCIS	Reliability Coordinator Information System
RRO	Regional Reliability Organization (SERC, NPCC, WECC, etc.)
RTO	Regional Transmission Operator
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
TCP/IP	Transmission Control Protocol / Internet Protocol
TPL	Transmission Planning
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Appendix E: Potential Responses to an Attack

Because attacks can come in different forms and attackers have different capabilities and motivations, it is impossible to prepare for them all. Each utility should create and execute a triage plan that will protect the most critical systems associated with real-time operations and situational awareness.

Listed below are a list of actions to consider based on the characteristics of the attack. These actions are broken up into the following categories:

- Voice and Data Communications
- Network Defenses (Internal and External)
- Operations (EMS/SCADA, Transmission, Generation)
- Information Sharing
- Forensics
- Personnel

Response Actions to Consider

- **Voice and Data Communications**
  - Determine impact to landline, VOIP and cellular communications as it relates to the Bulk Power System
  - Determine impact to ICCP, VOIP and other messaging data communications as it relates to Bulk Power System
  - Initiate satellite communication systems
    - Intra-communication to key power plants, etc.
    - Extra-communication to neighboring utilities, RC, RTOs, etc.

- **Network Defenses (Internal and External)**
  - Review password settings on key operational equipment and systems and knowledge of that information, and determine if possible modifications should be considered.
  - Check integrity of facility support systems (HVAC, water supply, physical access controls)
  - Review IDS/IPS and firewall settings to verify allowed access is still valid and required for current operating conditions.
  - Consider disconnecting external connections to business partners (e.g. VPNs or other point to point connections)
  - Remove all non-essential in-bound network access to control systems and related ESPs (remove support staff remote access)

- Remove all dial-up and remote command and control access links
- Implement IDS, IPS systems or FW rules that shun or block access attempts from source (if source info is provided)
- Review external network activity logs (especially for ESPs)
- Validate that only authorized access attempts are indicated in log files
- Tighten down host-based controls
- Temporarily change logging thresholds on key systems to capture more data for analysis

- **Operations (EMS/SCADA, Transmission, Generation)**
  - Review password settings on key operational equipment and systems and knowledge of that information, and determine if possible modifications should be considered.
  - Initiate emergency operations plans dealing w/ loss of communications and loss of control center functionality
  - Change control systems passwords for all systems deemed CCAs. Include non-CCAs as appropriate.
  - Remove contractor access to control systems and require escort access for all non-employees
  - Terminate control systems (EMS/SCADA) communication to the point that compromise is contained or rendered ineffective
  - Ensure EMS and State Estimation functions are operating properly. Validate and much as possible critical assumptions and values in database(s)
  - On a pre-determined schedule - Coordinate with Neighboring TOP/RCs on data validation points. Validation points are points where both entities have either independent monitoring or state estimated points from their own respective models. Both entities should be able to confer that based upon a predetermined set of validation points their respective state estimation and security analysis applications are both arriving at similar (not necessarily equal) values.
  - Disable EMS/SCADA control in a manner that preserves system stability while maximizing situational awareness for operators. (e.g. disable operator-initiated controls, followed by AGC if absolutely needed)
  - If disabling control fails to isolate the conditions, fully diable EMS/SCADA and operate power grid in manual mode by disabling all RTU communications. Disabling EMS/SCADA will hopefully preserve the state of the system forensic analysis.
  - Recover offsite backup tapes or “gold” copies of operating systems, configuration file, or applications for recovery purposes.

- Failover to backup control system(s)
- Contact your key hardware and application (including EMS/SCADA/Relays) vendors.
- Establish trigger points of distrust – i.e., if values diverge from one scan to the next by X% - attempt to validate value from other associated readings (i.e. are signals of large generation losses confirmed by changes in tie values). With such triggers, Operators should only take actions that can be validated at multiple ends via telecommunications.
- Work with vendor to develop/implement a solution (i.e. update firmware/software, replace compromised equipment with updated firmware, passwords, etc.)
- If attack corrupts primary and backup control center (BUCC) systems run off-line analysis from BUCC EMS packages and/or PSSE study files to validate outputs of control systems.
- Determine whether EMS Test environments can be leveraged in any way.
- Validate that only authorized access attempts are indicated in log file

- **Information Sharing**
  - Forward information (logs, backups, etc) to the ES-ISAC and/or ICS-CERT for further review and analysis. This includes any un-authorized access (electronic or physical) attempts.
  - Inform ISO/RTO/RC and neighboring utilities of incident
  - Contact local law enforcement for assistance with physical security
  - Actions could result in activation of NERC Crisis Plan and/or issuance of a NERC Essential Action Alert
  - Forward any evidence of related activity to ES-ISAC and *regional utilities* for further analysis and communication
  - System Operations and ESP Monitoring personnel should have frequent conference calls to correlate monitored ESP activity and system operations abnormal readings.
  - Utilize system "All-Call" and the RCIS to notify related operating entities of this activity and the need to consider validating readings and conducting conference calls to coordinate major system activities (i.e., opening lines, ramping down generation in a morning pick-up)

- **Personnel**
  - If unmanned, have a second shift man backup control centers.
  - If unmanned, deploy personnel to key substations, blackstart facilities and generation facilities

- All non-essential personnel shall be removed critical facilities (e.g. control centers, substations, generation plants)
- All affected facilities vital to the operation of the BPS should be staffed as needed by security trained and background checked individuals during the notice
- Co-locate Security Monitoring – or Cyber Incident Response team personnel with System Operations – so that the team can quickly assess suspect data/outputs and correlate it to ESP monitoring.
- Perform walk-downs of all critical facilities looking for abnormalities or unusual situations (tags on equipment maintenance ports are properly installed)
- Check seals on physical ports (i.e. maintenance ports) of programmable devices such as smart relays to determine if physical tampering has occurred.
- If “assigned” or “trackable” seals are used to manage access, validate seal information (i.e. serial number, scan code, etc.) to ensure that the proper seal is intact.

- **Forensics**
  - Preserve evidence to the extent possible (keep the system(s) in question in a state that allows for further forensic analysis).
  - All control system logs shall be maintained for 3 years for facilities that have CCAs (this includes non-impacted sites)

Appendix F: Precursors and Local Indicators of an Unusual Event

Some activities can be a precursor to the start of an actual event. While local indicators can happen routinely, having multiple occur could be a sign of an out the ordinary situation.

Precursors to Anomalies

- Reconnaissance activity on public facing web sites, with a focus on harvesting of email addresses or other contact information
- Correlated targeted malware delivery attempts (such as spear phishing) across the industry
- Correlated malware samples contained within the industry
- Observed anomalies along perimeter, guest, remote access or wireless networks
- Anomalies of outbound or egress traffic from highly controlled environments
- Public threats by activist or hacktivist groups
- Geo-political crisis

Anomalies in EMS/SCADA system application

- Displays not updating or erratic display update times
- Alarm “heart beat” fails
- Flurry of alarms determined by the system operator to be erroneous
- Flurry of alarms by State Estimator indicating a mismatch between field values and SE.
- Generator units not responding to AGC
- Not able to recover from a Control Performance Standard 1 and 2 excursion
- Large number of RTUs not available for scanning
- AGC or electronic dispatches not matching schedules
- ICCP in-operative
- Sporadic malfunctions of equipment or process

Anomalies in EMS/SCADA system hardware behavior

- High disk I/O rate
- Quickly diminishing free disk space
- High CPU utilization
- Undocumented service(s) running
- Slow network response
- Operator consoles loosing connection
- Change in network topology
- Unexpected network traffic
- Unexpected server(s) and firewall(s) restarts

- Unexpected loss of network connectivity, both internal and external
- Change in sound or pitch of equipment

Anomalies within Substations

- Alarms associated with relays, communications processors, SCADA
- Indications of physical access to equipment (tamper-proof tape on maintenance ports)
- Changes to relay configurations or settings
- Changes to ports/services on PCs or other equipment in substations (i.e. different from baseline)
- Changes to breaker settings or configurations
- Changes to RTU configurations or settings
- Passwords changed or checked out outside normal change cycle
- Alarms associated with devices unplugged or unauthorized devices connected to secured network (MAC addresses, switch ports normally turned down)
- Loss of RTU / DCS communication to the master EMS
- Change in sound or pitch of equipment

Anomalies in Situational Awareness

- Decrease in expected activity
- Similar activity as in previous hour, 24 hours or day that does not appear to match field readings
- Telemetry readings not matching schedules

Communication from (RTO and/or neighboring utilities, customers)

- Confirmed cyber security event at another entity
- Alarms associated with RTUs at interconnect points (multiple RTUs)
- Unconfirmed cyber security event
- Customer calls describing outages that do not correspond with normal alarms

Personnel

- Multiple personnel absent due to illness
- Erratic or nervous behavior
- Personnel missing or present during unusual times of during the day or shift

Appendix G: Isolation and Survivability Tactics

None of the suggested actions should be taken without first understanding the operational or situational awareness impact

Network Isolation

- Disable non-essential corporate connections to Internet, including e-mail
- Disable backup (dial-up or emergency) connections to Internet
- Disable connections with business partners (point-to-point connections and site-to-site VPNs)
- Disable remote access (dial-up, and client VPN) connectivity connections to internet
- Remove inbound connectivity to critical networks from corporate or business networks
- Remove outbound connectivity from critical networks to corporate or business networks to prevent further propagation

Operational Isolation

- Disable AGC and operate using local generator control
- Disable SCADA and Communications networks from Substations and Generation facilities
- Disable communications from Communications Processors in Substations from Intelligent Electronic Devices (IEDs) such as relays.
- Disconnect relays from breakers
- Islanding
- Under Frequency Load Shedding

Appendix H: Defensive Capabilities

Voice and Data Communications

- Telecom Companies (Cellular, POTS, etc.)– loss of RTUs, percentage thresholds
- Company owned copper – loss of RTUs, percentage thresholds
    - Have multiple path technology in place that could use several connection types / ISP's with the communications path using all that are available automatically.
- Multiple facilities/cell areas
- Cell phones / Smart phones – Social engineering, unsolicited inquiries
- Internet Service Providers detecting and dropping or rerouting malicious network traffic.
- Entity Owned Communication Networks (800 MHz, Microwave, Fiber, etc.)
- ICCP or Inter-Company Communications (Voice and Data)– loss of 2 or more simultaneously
- Satellite Communications
- Internal telecommunications facilities (e.g. ICCP.- microwave - local physical attacks (i.e. antennae structure damage)
- Dedicated facilities such as automatic ring downs (ARD) and Hotlines
- Social media – Twitter feeds, Skype, Facebook

Network perimeter defenses (border) – cyber intrusion into control center premise or critical asset premise

- Firewalls
- Intrusion Detection and Prevention systems
- Router Access Control Lists
- Data Diodes (or other methods of isolation – combination of routable and non-routable protocols)
- Vulnerability scanning and configuration management control (scans for changes in settings or configurations)
- Non-routable communications between servers
- Out of band communication to critical equipment (accessible over LAN/WAN and dial-up)
- Real-time logging of events on network and host devices.
- Alarms setup based on defined thresholds for abnormal events such as login fails, privileged account usage, or device probes that result in "access denied messages".
- Ability to query the log database for specific items that may not be in the current alarm pattern

- Security Information Event Management (SIEM) systems that consolidate logs and provide correlation of seemingly unrelated events,

Physical Defenses or Deterrence

- Motion detection – motion detector alarms, cameras, floodlights, control house intrusion alarms, loss of oil or over-temp transformer alarms
- Key card access
- Use of biometric controls
- Mantraps or other physical barriers that prevent tailgating
- Use of special locks for gates, equipment
- Increased patrols by law enforcement / contracted security
- Logging of physical access
- Increase access restrictions:
    - Advance notification for visitors
    - Limit access by outsiders to business need
- Increase use of security cameras, video surveillance.
- Staffing levels of key facilities
- Background checks
- Continuous behavioral monitoring
- Random drug testing

Generation Defenses

- Use of “Constant Frequency Operations” – previously defined for the Y2k transition.
- Use of “Conservative Operations” to maintain extra capacity
- Day-Ahead Planning – conservative mode unit commitment to maintain extra capacity and responsiveness
- Operation near unity power factor to maintain reactive capability (VAR reserves)
- Blackstart

Appendix I: CRPA Observations and Recommendations

Observations and Recommendations
Observation 1 - Most of the exercises and mini-programs included aspects of concurrent physical and cyber incidents, a tactic used to bring familiarity to the traditional domain of perimeter compromise to the assessment space. This use of mixed incidents was most prevalent when the participating entity migrated to Internet Protocol-based substation and SCADA operations. The goal was to determine general levels of readiness as they pertained to mapping physical asset break-ins to plausibly impact the cyber infrastructure. All entities had formal process and checklists to manage response to physical break-ins and theft of copper, equipment, and other valuable items. However, none had a process to consider if any technology had been *added* to the environment, such as rogue access points, radios, or other devices that could provide access to the EMS operational domain.
Recommendation 1 - Entities should update standard procedures for facility break-ins to include examination of systems for unauthorized changes to cyber assets. Additionally, entities should conduct system "sweeps" to identify any new equipment that may have been introduce to facilitate unauthorized access to the energy management command and control network.
Observation 2 - Most entities involved in the program had some form of cyber incident response plan in place or in development. In each case, the plans identified and assigned personnel and roles to respond to a cyber incident, but the plans lacked contingency planning in the event key personnel were not available. During the exercises and outreach campaigns, several participants noted that they were unfamiliar with the entire set of incident response activities, such as escalation, points of contact, impact analysis, etc. This observation suggests that, although a first-line of response had been established (and roles assigned), there was no capability to back-fill or cross-pollinate roles during a cyber incident. This issue can increase risk if, during an incident, trained personnel are not available and activities cannot be performed.
Recommendation 2 - The entire response team should be assigned primary and secondary roles, guaranteeing overlap in capabilities should the situation require it. Also, entities should include more group members from each response group in incident response training. This redundancy will provide some depth to the entity's "bench strength" and offer more resiliency. An entity should select a minimum number of people per department who should have incident response training, and ensure that those people receive the necessary training. Cross-train at least two additional staff members as incident response leaders who can take command of incident response activities.

Observation 3 - Having a corporate capability to interact with local and federal law enforcement during or after a cyber incident is something all entities deemed mandatory. While most organizations had at least one person in place that had some contacts in the law enforcement community, very little of their experience and knowledge had been internalized by the organization in the form of policies and procedures. After action reporting from exercise activity, combined with outreach and entity interviews, suggested that incorporating a law-enforcement communication function in the incident response plan would be useful, and that any experience and relationships entity personnel may have should be leveraged.
Recommendation 3 - Entities should work with local law enforcement to create a pre-populated list of law enforcement activities that could be performed during a cyber event. Establishing a pre-determined communication protocol with law enforcement entities would also be beneficial in helping to understand what law enforcement will do if called to support investigations. Feedback from participating entities suggested including law enforcement in exercise training activities, and proactively working with law enforcement to understand what is required should an actual incident occur. Entities should initiate a cooperative partnership with local Federal Bureau of Investigation or Royal Canadian Mounted Police offices, and include them in the response planning activities. NERC may wish to review any framework development that empowers BPS entities to create a law enforcement communication plan based on known investigative procedures, or suggest the augmentation of NERC CIP language to define the parameters that support law enforcement communications.
Observation 4 - During the exercises, interviews, and after-action discussions, the majority of participants appeared unsure about the necessary involvement of the RC in a cyber incident and are unsure how or when to engage them.
Recommendation 4 - Entities may wish to explore this issue further, as present protocols in place for interaction with RCs may not always include strategies as it pertains to a cyber incident where (a) reliability of BPS operation may be jeopardized, and (b) the communications path to the RC may be an attack vector. Entities are encouraged to work with their RC to establish a set of pre-defined incident response procedures which will determine when to include them in the communication chain during an incident. Moreover, NERC should investigate the protocol regarding entity-RC communications and reporting during cyber duress.

Observation 5 - The CRPA covers many aspects of entity operations and looks specifically at security operations for critical cyber assets; also included in the project activities were Primary Control Centers (PCC)/Main Control Centers and Back Up Control Centers (BUCC). A review of the findings indicates that, in many cases, the entity maintains BPS operations across a flat network and, to support redundancy, mirrors activities to a BUCC on that network. As the BUCC receives updates in real time from the systems in the PCC, a potential attack vector to the BUCC is established. Observations show that this architecture could create a situation where a cyber incident can impact mission critical backup data and critical cyber assets in the BUCC. The recovery protocol deployed suggests that should operators need to close the PCC and move to the BUCC, the operational environment at the BUCC would be useless as it has been compromised by association or archived (recovery) data is corrupted.

Recommendation 5 - Entities should consider expanding cyber protection measures to the communications infrastructure that support primary and backup facility operations. As it is assumed that all critical contingency communication resides behind and within the ESP, entities should consider monitoring the connection between the BCC and PCC for anomalous communications and other potential security-related events.

Observation 6 - The exercises showed that, while the technical teams were often quick to respond to the cyber incident (and begin their incident response activities), there were situations where no clear incident "leader" emerged to manage the incident on behalf of the whole organization. Key elements that were not coordinated included media relations, customer support, law enforcement, regulatory authorities and reporting agencies, and communications.

Recommendation 6 - Entities should continue to create and run incident response training exercises which include, and even focus on, management teams.

Observation 7 - The CRPA exercises, interviews, and after-action reporting demonstrated that the security architecture of vital transmission and distribution assets was constructed with significant security controls. Observers noted that assets are often managed by an internal team with a high level of skill and knowledge pertaining to BPS resiliency and EMS recovery. However, in many cases, the management of an entity's generation element(s) has been outsourced to third parties, resulting in increased response times, reduced control systems knowledge, and an impaired ability to manage energy assets in accordance with the entity's response protocols. These issues created extreme difficulty in managing fast-paced cyber incidents that include generation assets.

Recommendation 7 - Although these situations can be rare, the risk associated with insufficient security knowledge and response experience in the generation asset domain could prove to be significant during a cyber incident. Entities should consider moving management of all assets within the main EMS/SCADA and IT Engineering groups, resulting in an improvement to the overall management of generation assets.

Observation 8 - Despite the number of public displays of system compromise in recent years, combined with well-known cyber incidents impacting the energy sector, some individual participants remain skeptical about the possibility of a successful cyber attack on their own critical cyber assets, and as an extension, of the BPS cyber infrastructure itself. Participants did concede, however, that participating in scenario-driven exercises that used non-fictitious elements (cyber attack) to force them to test traditional response activities was very useful.
Recommendation 8 - As the threat and risk landscape can change quickly, entities are encouraged to incorporate specific intelligence about their operations into their planning and training agenda. In addition, as part of the risk assessment process, entities could extend their activities to determine actual and plausible threats against their cyber infrastructure and use that data to populate their exercise and training curricula. Training activities for SCADA/EMS operators should be expanded to include general cybersecurity training to all EMS/SCADA IT, Electric System Operations, Corporate IT, and IRT training regimens.

Appendix J: Case Studies

Breaking Air Gap Myths About Control System Inaccessibility - Stuxnet

Just because there is an "air gap" doesn't mean a control system is inaccessible to adversaries. Stuxnet is a great example. A USB thumb drive can be transported from an infected host machine and inserted into the target network that is air-gapped. Then stuxnet can propogate on the local target network via multiple exploits. That propagation results in forming a hostile Peer to Peer (P2P) network which operates on the probability of finding resident hosts with indirect or direct internet accessibility. It then utilizes these hosts to establish an indirect Command and Control (C2) bridge for hostile control. In sum, USB served as not only the delivery mechanism but also to establish a network of hostile P2P relationships within the target network.

Another Example, Breaking Air Gap Myths About Control System Inaccessibility – Buckshot Yankee

SIPRNET is Department of Defense's (DoD) Secret-level network. This network is commonly perceived as completely air-gapped, yet in 2010 Deputy Defense Secretary William Lynn publicly disclosed a 2008 worm infestation on the network. The DoD response to this infestation was called Buckshot Yankee. Also in 2010, well-known former counter terrorism official Richard Clarke released a book entitled "Cyber War." Clarke gave a more detailed account of Buckshot Yankee. The delivery mechanism was USB insertion, much like stuxnet, but its C2 method was novel. Instead of P2P C2, Buckshot Yankee relied on sneaker-net C2. The infected thumb drive payload carried not only the malware worm but also a data file. This data contained requests and responses which serve as a C2 channel to the next internet connected devices the USB is inserted into. The result: USB creation of an effective hostile sneaker-net C2 channel across the perceived air gap which "secures" the target network. The bottom line: USB established a delivery mechanism within an air-gapped network and then sneaker-net connectivity enabled by repeated usage of USB devices between both air-gapped and non-air-gapped networks.

TAKE AWAY, what these examples say about Cyber Attack awareness…

Techniques such as utilizing USB devices as delivery mechanisms to enable hostile penetration of targeted "secure" control networks is widely known. Approaches of establishing hostile C2 channels across the gap using techniques such as P2P or sneaker-nets are less well known.

Techniques like these mean that defensive measures limited to reliance on air gaps need to be evaluated skeptically. Other advanced and novel means of hostile penetration, and the means to offer effective layered defense against them, must be considered to achieve true control network and device security and true risk management. These observations point towards integrated consideration of policies, procedures, system design, operational approaches, intrusion detection, anomaly, monitoring and awareness technologies which deliver a capability

to understand own network health, vulnerabilities and mitigation options. Take a proactive and more informed view towards the challenges and opportunities to enhance your security by keeping apprised of hostile techniques, tactics and procedures (TTP) like the two illustrative examples above.

Disruption through swarming

Creating an open call for volunteers in an ad-hoc, extemporaneous way to do something is popularly known as crowd sourcing. It's leaderless or structure-less network of people coming together for a common purpose and then disbanding. Adversaries use this tactic. The Anonymous (a loose knit global hacktivist group) hive is the personification of this but there are others.

In 2008, at the onset of war between Russia and Georgia, a distributed denial of service attack (DDoS) began against government websites. As hostilities began, this was extended to Georgian media websites covering the hostilities. These various DDoS attacks lasted for hours and had a peak of over 800Mbps. A few months later an analysis under the moniker of "Project Grey Goose" was released. This report outlined the coordination ground for these DDoS to a website called stopgeorgia.ru. This was a password-protected forum launched within 24 hours of hostilities. These DoS attacks were interspersed with website defacements posting pro-Russian propaganda.

These DoS activities and defacements were seemingly self-organized or crowd sourced on sites such as stopgeorgia.ru. Many believe the Russian government was in the background of these pro-Russian hackvists. At the very least, the Russian government appeared to condone the activities as evidenced by their clear restraint in not launch any investigation of the attacks.

Anonymous uses surprisingly similar tools to organize (online forums) - and similar tools to launch attack activity (denial of service attacks). Their tool of choice is called Low Orbit Ion Cannon (LOIC). LOIC is an application designed to launch DDoS attacks. LOIC by itself is uninteresting. It's the forums that are interesting. You'll see a long list of independently organized "operations" or "ops". Each of those operations are public and open to the community to comment on. There are dozens of ops at any given time, most of them become background noise. Others take off and develop a life of their own. The HBGary Saga is a good example of a successful op. But for each successful op there are countless that don't see the light of day. Combine this with the LOIC tool: when you give it to the hands of 10,000 who point it at the same target then you have a distributed denial of service. This is what was used in Operation Payback when Anonymous attacked PayPal and others after they refused to provide services to wikileaks.

This is a noteworthy tactic as indications are that it is employed by a wide range of adversaries. Pro Russian groups used it as a propaganda and disruption tool, and Anonymous continues that tradition.

TAKE AWAY is that swarming is a practice that has been observed, Crowd sourcing and social media techniques are easily available to motivated groups that may seek to use them for distributed denial of service disruption.

Off the shelf tools

There exists an ecosystem of tools available to the adversaries. Some of these are dual use for offensive and defensive purposes. Some of these tools are merely used at research levels, others for active attacks. Fuzzing tools and Security debugging tools such as olly or ida pro - which are development environments. These can pinpoint flaws in software and ultimately lead to exploit code that can be weaponized.

LAMP stands for Linux Apache Mysql and PHP. It is a "vanilla" OS, Webserver, SQL server and a web application language and how those four off the shelf technologies can be combined for rapid web development. LAMP is the model being packaged and sold by malicious underground adversaries in order to exploit people. These are known as exploit kits. Exploit kits use LAMP to set up malicious web pages, and use those pages to attack web browser and client components. The exploit kit also keeps track of the overall success rate. The kits create malicious iframes that will attempt to use a series of several exploits all at once in order to execute a malicious payload on the target machine. These iframes are windows cut into the webpage that allow visitors to view another page on the site or off the site without reloading the entire page. The exploit kit will also track victims by IP address, country, browser, OS-level, etc…

These malicious pages are delivered through vectors such as search engine optimization (SEO) and Phishing attacks.

Contagio dump (a web based collection of the latest malware samples, threats, observations and analyses) is tracking 64 versions of 42 unique exploit kits in the wild. Most of these contain between 10-20 exploits and each kit is sold for between $1000 to $2000. These 64 unique exploit kits have a total of over 100 unique exploits! Mostly targeting flash, adobe, quicktime, java, or browser vulnerabilities. Tools other than exploit kits also exist. LOIC is another off the shelf tool to be aware of. Additionally, there are Trojans, such as poison ivy, zeus, TDL, and others, which threat actors can purchase or gain use of through underground or criminal communities.

TAKE AWAY is that exploit kits are ubiquitous and inexpensive for criminal groups to obtain and utilize. Software development quality control and layered defense in depth, combined with own systems awareness are key defensive measures.

Lateral Movements

Adversaries with long-term motives will typically focus in on first gaining access to a target network, then finding target hosts on the network which enable network understanding. This tactic is generically referred to as moving laterally in the compromised network. This is where it can be tough to remove an adversary on your network because the adversary is in several places.

The tactic - and both Google Aurora as well as the RSA breaches saw this tactic used - starts with patient zero. Once patient zero is compromised the adversary begins compromising other workstations or servers with back doors. Adversaries will then use those backdoors and stand up their operations. One workstation may host various attacker tools: another workstation will be for data staging if the aggressor plans on finding and exfiltrating data. Yet another box is simply given a back door and not touched in case the aggressor loses access to the other boxes. Aggressors may continue lateral movements as they seek long-term objectives and escalate priviledges on the network.

Lateral movement typically occurs through a technique such as Passing the Hash. To illustrate, if an attacker gains access to a target user workstation and the user happens to be a local administrator, the goal becomes to jump from this springboard workstation to a print server and plant a “back door.” This is convenient because the attacker already knows the print server hostname since the user has access to it. What might not be known to the attacker is the target user domain password nor whether hi account has access to interactive sessions with the print server. Attackers may rely on the fact that Windows has a core OS service running known as Local Security Authority. This service caches the users and associated password hash data after a user has authenticated to the local system. The adversary can then utilize a tool known as Wondows Credential Editor (or metasploit…) and dump password hashes. This is not the plain text password. The password is not needed. Wondows Credential Editor can utilize this NTLM hash and start processes as the attacked user. The attacker uses Windows Credential Editor and dumps the cached hashes in LSA. The attacker identifies an account called “service Veritas.” That shines out to the attacker because Veritas is a backup software solution. If the backup software is using this service, there is a high likelihood that it is domain admin or nearly equivalent. Windows Credential Editor allows the attacker to use this hash and pass it on to the system to run processes as that user. On the local machine, he can then remotely connect to boxes as that service account. That’s how backdoors can be planted. Subsequently, one could come back to the print server and list hashes that are cached on the print server. If the domain equivalent user has recently talked to the print server, that hash can be stolen and used as an attacker enabler for easy internal movement within the target network environment.

TAKE AWAY is that a foundational defensive element of strategy for every organization should be development and maintenance of own asset and own system baseline configuration and operational states, as well as own systems operational awareness. Obtaining and keeping good forensic and log data can be very crucial to effective and sustainable defensive posture. Often a few Indicator of Compromise (IOC’s) can be developed around a few key, but important, departures or anomalies from normal operating parameters. These can be used to identify and triage attempts at compromise.

Appendix K: Task Force Goals and Objectives

The goals and objectives of the CATF are:

Goals	Objectives
Review current situation and capabilities	1. Consider the ability of entity system operators and cyber security analysts to detect and respond to a coordinated cyber attack. 2. Consider the extent to which entities may not isolate critical cyber systems from other business or Internet-facing systems, and the extent to which this increases the vulnerability of their systems. 3. Consider opportunities to isolate, prevent further propagation, or otherwise protect cyber systems and bulk power system assets. 4. Consider the capabilities of voice and data communications tools and energy management systems, with a focus on which minimum functional needs system operators must retain and the alternative methods to acquire or maintain this capability even in a reduced state. 5. Consider staffing capacity, challenges, and safety. 6. Assess the adequacy of current CIP cyber security practices under a coordinated cyber attack scenario.
Perform needs assessment	7. Identify the functions needed to support reliable power system operations that would be particularly challenged under a coordinated cyber attack scenario.
Develop alternative solutions	8. Assess the options, benefits, and costs associated with isolating critical cyber systems (i.e. control systems, energy management systems, protections systems, and their networks). Consider complete or virtual (e.g. virtual private network) separation. 9. Propose a range of alternative solutions to enhance operating capabilities, including estimated costs and effort to develop and maintain this capability. Identify the residual

	risks that may be associated with each of these solutions.
Coordinate Solutions	10. Assist in outreach efforts to educate regulators, organizations, and other infrastructures in better understanding the electricity sector's preparations to address these threats.
Recommend Solutions	11. Recommend potential practices or programs for use by NERC or individual entities. Create scalable drill templates that registered entities could utilize to train personnel and enhance current restoration and operating protocols.