EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Guidelines for Leveraging NESCOR Failure Scenarios in Cyber Security Tabletop Exercises

December, 2014

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

Principal Investigator
T. Overman

EPRI Authors
A. Lee
G. Rasche
T. Overman

This report describes research sponsored by EPRI.

EPRI would like to thank all the individuals who worked on the NESCOR failure scenario documents. Their commitment and dedication resulted in documents that are very useful to the electric sector. Some of that information is included in this report.

CONTENTS

TABLES

FIGURES

1
EXERCISE FACILITATION PLAN

1.1 Purpose and Scope

This document provides exercise facilitators with guidance concerning procedures and responsibilities for exercise development, facilitation, simulation, and support. It explains the exercise concept as it relates to facilitators, establishes the basis for facilitation and simulation of the exercise, and establishes and defines the communications, logistics, and administrative structure needed to support facilitation and simulation during the exercise. This document includes a National Electric Sector Cybersecurity Organization Resource (NESCOR) failure scenario and explains how to expand this scenario for use in a cyber security tabletop exercise.

1.2 Primary Source Documents

This document was developed by the Electric Power Research Institute (EPRI). Portions were adapted from material provided to the public by the U.S. Department of Homeland Security (DHS) [10,11], Federal Emergency Management Agency (FEMA) Emergency Management Institute [1,2,3], the Homeland Security Exercise and Evaluation Plan (HSEEP) [4], the North American Electric Reliability Corporation (NERC) [5,6,16,17], the National Institute of Standards and Technology (NIST) [12,13,14,15], NESCOR [7,8,9], and EPRI. Although the FEMA materials cover both tabletop and full-scale field exercises, this document is limited to cyber security tabletop exercise planning. Tabletop Exercises are referred to in this document using the abbreviation TTX [1].

1.3 Single-site vs. Multi-Site Tabletop Exercises

Single-site tabletop exercises are much simpler to conduct than multi-site exercises. Facilitator(s) can adjust the timeline of information injects from the Master Scenario Event List according to the actual flow of discussion among the players. Multi-site tabletop exercises, however, take more care in planning and close coordination between facilitators during the exercise. Information injects must be synchronized carefully according to the needs of the scenario development.

This facilitation plan addresses both single-site and multi-site exercises. When developing plans for a single-site exercise, planners may eliminate content and complexities which are not needed.

1.4 Play Concept

This section provides an overview of the exercise and related exercise activities, a general description of the scenario, an overview of primary players and their exercise locations.

1.5 Overview

Exercise play should officially begin and end per a defined schedule. The exercise will be played for approximately three hours. On the scheduled date, the exercise will be initiated by a 30-minute orientation briefing. The briefing should include a review of current operational status, whether there are conditions with the potential to impact operations, and background actions that

have been taken by incident response organizations. This background briefing will be based on the information in the Scenario Narrative. A 30-minute hot-wash review will immediately follow the exercise. There will be a post-exercise meeting a few weeks after the exercise.

1.6 Exercise Facilitation Team Staffing

Personnel selected as exercise facilitation team members must be knowledgeable of operational incident management and response functions of the system(s) that are the focus of the exercise. Personnel need this knowledge to understand ongoing exercise activities and to be able to track them with events in the Master Scenario Event List (MSEL). For these tabletop exercises, smaller scale than regional or national events such as GridEx, the facilitators may be selected from the exercise planning team.

1.7 Exercise Facilitation Team Roles and Responsibilities

[The following material is extracted from the FEMA Emergency Management Institute Independent Study Course (IS) 139 Exercise Design, *Exercise Control Plan* document with some minor revisions.]

At a minimum, all participants (facilitators, players, observers) should receive an orientation briefing and handout materials that cover the exercise plan, including scenario, objectives, procedures, and ground rules. Facilitators should conduct this briefing ahead of the day of the exercise. Facilitators should conduct another briefing, more focused on the exercise narrative, on the day of the exercise.

Facilitators must understand the following.

- Purpose and objectives of the exercise.
- Master Scenario Event List and scenario time line.
- Message forms and flow of information.
- Content of exercise messages.
- Accuracy, timeliness, and realism of expected responses.
- Requirements for coordination with observers and other personnel.
- Procedures and communications methods for injecting messages.
- Procedures for monitoring the sequence of events and message flow.
- Procedures for controlling spontaneous exercise inputs and for responding to unplanned or unexpected situations.
- Procedures for recording and reporting exercise information.
- Procedures for post-exercise debriefings and evaluation.

This section identifies the responsibilities of the lead Facilitator as well as those (for multi-site exercises) of the facilitation team for each site.

Prior to the exercise, all exercise facilitation personnel should be familiar with this facilitation plan. They should also be familiar with the exercise MSEL events, especially those to be injected into play from their assigned location.

1.7.1 Lead Facilitator/Assistants

The lead facilitator is responsible for managing and directing all facilitation and simulation functions during the conduct of the exercise. He/she may be assisted in this function by one or more individuals. Specifically his/her responsibilities include the following:

- Participate in the exercise design team.
- Analyze and assess the exercise plan to determine an appropriate facilitation strategy (location of facilitation sites and simulation cells, number of personnel required, roles and responsibilities, etc.).
- Develop and disseminate the exercise facilitation plan.
- Establish Facilitator/simulator communications systems and information support mechanisms.
- Design and develop the facilitation organization and chain of command (for multi-site exercises).
- Define the role and responsibilities of the exercise facilitation team.
- Develop policies, guidelines, and procedures for implementing the exercise facilitation plan.
- Develop the administrative and logistic systems needed for reporting, problem resolution, and safety and site preparation for participant organizations and Facilitators.
- Determine the qualifications and experience level of facilitators needed and identify avenues for obtaining them.
- Design and develop training for exercise facilitators.
- Develop procedures for debriefing players and the exercise facilitation team.
- During the exercise, manage and coordinate activities of the exercise facilitation team to ensure that exercise play achieves exercise objectives.
- Direct corrective actions to exercise play, if required.
- Monitor exercise progress and make decisions regarding any deviations or significant changes to the scenario caused by unexpected developments in the course of play.
- Conduct a debriefing of exercise facilitation team.

1.7.2 Site Facilitation Lead Responsibilities

Note: For some organizations, exercises will be multi-site but facilitated from a single location. Instant messaging, web collaboration, email, or similar collaboration tools should be used to enable a facilitator from a central location to communicate with groups of players and observers at remote locations.

For a multi-company TTX, site facilitation team leads are responsible for managing the facilitation functions at a specific site. During exercises in which all facilitators are located at a single facility, this role is usually filled by the lead facilitator. For complex exercises, multiple facilitation team leads may be necessary. Therefore, in some situations, these duties may be separate and distinct or fulfilled by one person.

The person in charge of facilitators at each primary location will be referred to as the facilitation team lead and will be responsible for directing all functions of his/her respective team. Specifically, each facilitation team lead's responsibilities include the following:

- Review facilitation plan and attend facilitator training.
- Assist with training and briefing of the exercise facilitation team.
- Present ground rules to exercise players.
- Manage all exercise facilitation activities at the assigned exercise location.
- Ensure that site preparations are complete.
- Monitor and report exercise activities at the assigned location, including flow and pace of the exercise.
- Track the accomplishment of exercise objectives and apprise the lead facilitator regarding any deviations or significant changes to the scenario caused by unexpected developments in the course of play.
- Coordinate facilitation activities with the facilitation team leads at other exercise locations as required, keeping the lead facilitator informed.
- Ensure the safety of exercise participants.
- Coordinate any required modifications to the MSEL and supporting event implementers with the evaluation team leader at the exercise location and with the lead facilitator.
- Maintain records of all ad hoc implementer messages created by facilitators and injected into exercise play.
- Provide observations for input to the exercise evaluation using the key player observation and comment form.
- Complete routine reports to log exercise events and any special reports, as necessary.
- Chair the post-exercise critique session/hot-wash review at his/her location.
- Attend facilitation team debriefings.

1.7.3 Exercise Facilitation Team Interaction Procedures

For both single-site and multi-site exercises, the facilitation team members will have constant interaction with each other, and with the players. Facilitators monitor and manage exercise activities to ensure that exercise events occur in sequence and at the proper time to meet exercise objectives. Observers view exercise activity and gather information during the exercise for the exercise After Action Report and Improvement Plan. The following paragraphs describe the procedures associated with their interaction.

1.7.3.1 Interaction between Facilitators and Observers

The evaluation of the objectives for the exercise will be managed and conducted by the planning team, who will gather information during the exercise by direct observation of player activities. Exercise facilitators must be proactive in monitoring events occurring in the exercise at their location and with related events at other locations.

1.7.3.2 Interaction with Players

Facilitators should have constant interaction with players throughout the exercise; however, each interacts differently. Facilitators interact with players by following the MSEL and injecting implementer messages. Facilitators also interact with players as required to ensure the flow of the exercise and that exercise objectives are being met. Facilitators must ensure that they do not disrupt play when communicating with the players.

1.7.3.3 Interaction between Facilitators during multi-site exercises

Facilitators should have constant interaction. Facilitators will inject the event implementers in accordance with the MSEL. Anytime a Facilitator receives a question from a player that requires response from a nonparticipating organization or person, the facilitator should exercise judgment and provide a response that the participant would be likely to receive from their staff

Many MSEL items require the coordination between and among exercise sites. Therefore, it may be necessary during the course of play for facilitators at one location to contact facilitators at other player locations. For example, many MSEL items identify related events that need to occur prior to their injection. In some exercises, these related events may take place at different locations. Prior to injecting an MSEL item of this type, the facilitator should ensure that the related events that need to precede it took place by contacting the facilitator at the location injecting the MSEL item. When a related MSEL event does not occur, facilitators at both locations need to coordinate and develop a corrective action. Corrective actions may consist of direct coordination by a facilitator with an exercise player to determine the status of an action, possible deletion of an action because it has been overcome by events, or development of an ad hoc event implementer message. All corrective actions should be coordinated.

1.7.4 Problem Resolution Procedures

There may be times during an exercise that problems will arise that cannot be resolved by a particular facilitator. Site facilitators are advised to discuss these problems with the Lead facilitator during multi-site exercises. Resolution might include modification of the MSEL. The following two paragraphs describe the procedures that need to be followed to modify the MSEL during an exercise.

Deletion of MSEL Events

In some cases, the course of exercise play may make some MSEL events inappropriate or unnecessary. In those instances, facilitators may, with the concurrence of the lead facilitator, delete an MSEL event entirely or postpone it until a later time. Facilitators must ensure the deletion of the MSEL event does not affect actions at other locations (for multi-site exercises) that require it as an action stimulant. Therefore, coordination is required from the lead facilitator. Records of coordination and the MSEL

event deletion must be maintained for later use during the After Action Report and Improvement Planning phase.

Addition of Ad Hoc Implementer Messages

In some cases to maintain the pace and momentum of exercise play or to cause an expected player action to occur, facilitators may find it necessary to inject an event implementer that was *not* envisioned during exercise design. This type of unplanned message is called an ad hoc implementer. Facilitators may, with the concurrence of the lead facilitator, insert an ad hoc implementer message to induce or replace the required player action, duly recording the circumstances. Facilitators should record development and use of the ad-hoc message.

1.7.5 Post-Exercise Critique Session/Hot-Wash Review Procedures

A 30-minute post-exercise critique session, called a hot-wash, will be conducted at each exercise location following termination of exercise play. The purpose of this session is to solicit immediate feedback from exercise participants on how the exercise went including whether or not the objectives were met), and to identify areas that will require attention, areas that functioned well, problems encountered, etc.

The facilitator at each location is responsible for chairing the hot-wash session. He/she will obtain overview information and feedback forms from players and observers.

1.7.6 Exercise Planning and Facilitation Team Debriefing Procedures

Immediately following the exercise and the hot-wash session, the planning and facilitation team will conduct a more detailed internal debriefing. All planners and facilitators should prepare for the debriefings by compiling their logs and MSEL notes. The debriefings may focus on collecting the following types of information.

- Were there areas that player exercise performance was commendable?
- Did you notice areas that require improvement?
- Were actions or decisions made that were not consistent with plans or procedures?
- Did you see any major problems that would affect the participating organization/department's ability to respond to a cyber security incident?
- Do you have any recommendations on what can be done to improve exercise facilitation?
- Did you have any specific problems with exercise facilitation?
- Do you feel that there was sufficient time for exercise play?

This information will be used as the basis for the After Action Report and Improvement Planning process.

2
SCENARIO NARRATIVE DEVELOPMENT

2.1 Step 1: Identify existing plans/policies/procedures to be tested

The heart of a cyber security TTX is the testing of an organization's plans, policies, and procedures for incident detection, response, and recovery. Consequently, the first step is to identify and review which of these are to be tested. Most organizations have a variety of plans related to information security. These plans, policies, and procedures are often a combination of both enterprise-wide and department-specific documents that are coordinated.

For the cyber security TTX, the focus is on the document and the related department-specific cyber incident response plans for the organizations identified in Step 2 below.

2.1.1 NERC CIP Tabletop Exercise Consideration

Some tabletop exercises may be developed that are intended to satisfy the North American Electric Reliability Company (NERC) Critical Infrastructure Protection (CIP) requirements. When doing so, the exercise planning team should review relevant sections of the NERC CIP documents. At a minimum, the following NERC CIP references (or equivalent references) should be addressed.

1. CIP-008-5 – Cyber Security – Incident Reporting and Response Planning [16] Requirement 2.1 states:

   "Test each Cyber Security Incident Response plan(s) at least once every 15 calendar months:

   - By responding to an actual *Reportable Cyber Security Incident*;
   - With a paper drill or tabletop exercise of a *Reportable Cyber Security Incident*; or
   - With an operational exercise of a *Reportable Cyber Security Incident*.

   Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises."

2. The Glossary of Terms Used in NERC Reliability Standards [16] defines a Reportable Cyber Security Incident:

   "A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity."

2.2 Step 2: Identify the components of the enterprise that will be involved in the TTX

An electric utility may choose to have an enterprise-wide exercise, in which Information Technology (IT) or Operational Technology (OT) systems in all business areas are impacted or need to be analyzed in some manner. In other exercises, a TTX may focus on a few departments or locations.

- As an example, for the TTX the scope includes:
    - [Energy Management System (EMS1)]
    - [Generation Station 1]
    - [EMS2]
    - IT Data Network

2.3 Step 3: Review NESCOR Failure Scenarios for applicable Scenarios

Review the list of Failure Scenarios in [7], particularly the subset of scenarios identified later in this section. Select one or more scenarios based on the internal processes to be exercised, and the technology area or department selected to be the focus of the exercise.

2.4 Step 4: Develop Scenario Narrative

Once Steps 1, 2 and 3 above are completed, the plans/policies/procedures of the applicable components should be reviewed to identify areas where specific actions are expected based on some type of pre-determined criteria. At the same time, a scenario narrative can be developed that outlines at a high level the types of cyber security actions by insiders (inadvertent or intentional) and by outsiders (inadvertent or intentional), which could have a detrimental impact on the organization's ability to continue providing reliable electric service.

2.5 Using the NESCOR Failure Scenarios for Tabletop Exercises

Scenario details from [7,8,9] are an excellent source of information for a scenario narrative. These scenario details are also useful for guidance when developing a more detailed Master Scenario Event List. The details can be used to inform incident response actions; test current plans, policies and capabilities; and explore areas for improvement planning after the exercise.

In [7], the failure scenario *Description*, *Impact,* and *Potential Mitigations* sections are of particular interest. These can provide players with context for questions to ask of their staff. For example, AMI.12 lists the following in addition to other Potential Mitigation actions.

- *Detect unauthorized access* between Internet and AMI consumer information
- *Create audit logs* of firewall rule changes and customer database accesses
- *Detect unusual patterns* of database access

During an incident (and during the tabletop exercise), requesting information from the audit logs of firewall rule changes, or of database access can be used to find the root cause of the incident. This information can also inform corrective actions. If support staff is unable to provide log

access details in a timely manner, this may be an area for improvement after the exercise is finished.

2.6 Scenario Narrative Comparison to GridEx I and GridEx II

As shown in the GridEx After Action Reports [5,6], the scenario narratives for those exercises were complex and several pages long. For the smaller-scale exercises anticipated under this set of planning documents, the scenario narrative will be shorter – at most a few paragraphs of text. The scenario narrative should outline the basic failure scenario in a way that will enable players to anticipate and bring with them any relevant materials, including organization and technology-appropriate incident response plans that their department/organization utilizes.

2.7 Failure Scenarios to Consider

The NESCOR Electric Sector Failure Scenarios and Impact Analysis document [7] was referenced for this scenario development aspect of tabletop exercises.

The focus of a cyber security tabletop exercise is reviewing plans and procedures for incident detection and response. Consequently, planners are encouraged to select scenarios with strong emphasis on policies and procedures, rather than failures scenarios with mitigation activities more focused on technical countermeasures. Using that as the ranking criteria, NESCOR Failure Scenarios particularly well suited to use in tabletop exercises include the following.

1. Advanced Metering Infrastructure (AMI)
    a. AMI.2 Authorized Employee Manipulates MDMS Data to Over/Under Charge
    b. AMI.9 Invalid Disconnect Messages to Meters Impact Customer and Utility
    c. AMI.13 Authorized User uses Unattended Console to Disconnect Customer
    d. AMI.15 Inadequate Security for Backup AMI Enables Malicious Activity
    e. AMI.24 Weak Cryptography Exposes AMI Device Communication
2. AMI.25 Known but Unpatched Vulnerability Exposes AMI Infrastructure Distributed Energy Resources (DER)
    a. DER.1 Inadequate Access Control of DER Systems Causes Electrocution
    b. DER.2 DER's Rogue Wireless Connection Exposes the DER System to Threat Agents via the Internet
    c. DER.3 Malware Introduced in DER System During Deployment
    d. DER.5 Trojan Horse Attack Captures Confidential DER Generation Information
    e. DER.10 Threat Agent Modifies Field DER Energy Management System (FDEMS) Efficiency Settings
3. Wide Area Monitoring, Protection, and Control (WAMPAC)
    a. WAMPAC.4 Measurement Data Compromised due to Phasor Data Concentrator (PDC) Authentication Compromise

b. WAMPAC.5 Improper Phasor Gateway Configuration Obscures Cascading Failures

c. WAMPAC.12 GPS Time Signal Compromise

4. Electric Transportation (ET)

    a. ET.3 Virus Propagated between Electric Vehicles (EVs) and EV Service Equipment (EVSE)

    b. ET.12 Unavailable Communication Blocks Customer Use of EV Preferential Rate

    c. ET.14 EV Charging Process Slowed by Validation Delay of EV Registration ID

    d. ET.16 An EV is Exploited to Threaten Transformer or Substation

5. Demand Response (DR)

    a. DR.2 Private Information is Publicly Disclosed on demand response automation server (DRAS) Communications Channel

    b. DR.3 Messages are Modified or Spoofed on DRAS Communications Channel

    c. DR.5 Non-specific Malware Compromised DRAS or Customer DR System

    d. DR.7 Custom Malware Compromises Customer DR System

6. Distribution Grid Management (DGM)

    a. DGM.1 Wireless Signals are Jammed to Disrupt Monitoring and Control

    b. DGM.2 Shared Communications Leveraged to Disrupt Distribution Management System (DMS) Communications

    c. DGM.3 Malicious Code Injected into Substation Equipment via Physical Access

    d. DGM.4 Malicious Code Injected into Substation Equipment via Remote Access

    e. DGM.5 Remote Access Used to Compromise DMS

    f. DGM.8 Supply Chain Vulnerabilities Used to Compromise DGM Equipment

    g. DGM.9 Weakened Security during Disaster enables DGM Compromise

    h. DGM.10 Switched Capacitor Banks are Manipulated to Degrade Power Quality

    i. DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System

    j. DGM.15 Threat Agent Causes Worker Electrocution via Remote Access to Distribution System

7. Generic

    a. Generic.1 Malicious and Non-malicious Insiders Pose Range of Threats

    b. Generic.2 Inadequate Network Segregation Enables Access for Threat Agents

    c. Generic.3 Portable Media Enables Access Despite Network Controls

d. Generic.4 Supply Chain Attacks Weaken Trust in Equipment

2.8 Simulated failure of business network

Many types of tabletop exercises, such as those considering storm preparations, earthquake response, or civil unrest, include degradation and loss of normal communications as part of their scenarios. These cyber security tabletop exercises will do the same, but based on the generally accepted risk profile of corporate business networks as compared to control system networks.

The main focus of a cyber security tabletop exercise scenario is on control systems and functionality. In most enterprises, the business computing environment is used extensively for off-line review of control data using data historians, and for normal business communications and coordination. Over the past several years, the use of Voice over IP (VOIP) telephones has become more common. Business data networks are typically used to coordinate incident response. Because these business networks are also likely to be impacted by a cyber security incident, it is recommended that failure of the business network should be a component of any cyber security tabletop exercise.

3
MASTER SCENARIO EVENT LIST DEVELOPMENT

3.1 Master Scenario Event List (MSEL) Development Overview

[The following two paragraphs are extracted from the FEMA Emergency Management Institute Independent Study Course (IS) 139 Exercise Design, *Exercise Control Plan* document.]

> The exercise will be controlled by the Master Scenario Events List (MSEL), which is the primary document used by facilitators to manage the exercise, to know when events are expected to occur, and to know when to insert event implementer messages into the exercise. In other words, the MSEL provides the framework for monitoring and managing the flow of exercise activities. The MSEL is restricted for use by facilitators and observers.
>
> The MSEL is the collection of exercise events that support the exercise scenario, exercise objectives, and points of review. The MSEL includes events that are player actions, and events that must be injected by facilitators. All events listed in the MSEL are in chronological sequence. Weather-related information injects, which may impact expected local or regional electrical loads, are included in the MSEL. Facilitators will use the MSEL in this form to monitor and manage exercise flow.

For half-day cyber security tabletop exercises there should be no more than 25 events on the MSEL. Some events in the MSEL will be injected after a lengthy delay from the prior event. Some events will be injected into exercise play in rapid succession.

The main focus of a cyber security tabletop exercise is a review of incident detection, response, and recovery plans, procedures and capabilities. Ensuring achievement of the exercise objectives is more important than strict adherence to the MSEL and covering every planned scenario event. Scenario event sequence is important, so events should not be skipped over. However, during the conduct of the exercise, it is likely that not all scenario events will be injected. Facilitators will have to use care and judgment in determining when to pull exercise players back from productive discussion of existing plans, and when to move exercise play forward by injecting the next event from the MSEL.

Because a tabletop is only partially simulated, it requires little scripting. The only roles are the facilitator, the players (who respond in their real-life roles), and one or two observers. Observers take minutes and record decisions and usually do not need formal evaluation forms.

It is a non-trivial activity for exercise planners to take a scenario from the NESCOR documents and create the MSEL details. This step will require company-specific

knowledge of the systems that are implemented and how/where the systems interact with each other.

In developing the MSEL, it is important to remember that the purpose of the exercise is to work with existing plans and procedures used to detect and address cyber security incidents. Among the items to consider are:

1. Issues with identifying a cyber incident versus a communication or sensor failure;
2. Problems determining if a cyber incident is malicious or non-malicious;
3. The impact of a blended cyber-physical attack (if the exercise scenario includes both cyber and physical system attacks); and
4. Addressing an 'intelligent adversary' that can respond to your actions, etc.

3.2 Master Scenario Event List (MSEL) Data Fields

[The following material is extracted from the FEMA Emergency Management Institute Independent Study Course (IS) 139 Exercise Design, *Exercise Control Plan* document.]

The following paragraphs describe each MSEL component in greater detail and any procedures involved with a particular component.

Event Number

The event number is a unique number assigned to each event. The current numbers assigned to each event represent a chronological sequence of events. This number will not change. MSEL tracking is facilitated by maintaining the original MSEL event number. The numbering scheme is multi-part. The first digit is the "Move" which is the main section of the exercise:

Move 1: Identify Cyber Incident from normal system failure

Move 2: Contain Cyber Incident

Move 3: Mitigation/Recovery

The second part of the Event Number is just a one-up increment counter.

Inject Time

The inject time is the time when the Facilitator is expected to inject the event implementer into exercise play. Facilitators must monitor inject times closely, especially during multi-site exercises. If, after a reasonable time, an expected player action has not occurred, Facilitators may consider prompting the action. This is especially true for the first few events, while the players are just getting started. If the "Inject Time" is not compatible with ongoing exercise play as it is occurring, the facilitators may delay injecting the event implementer until the appropriate time (or inject it sooner if necessary).

From The "From" field is the organization or individual from whom the event implementer is being sent.

To The "To" field is the organization or individual intended to receive the information contained in the event implementer. This is the person or organization that the Facilitator will call/write/see to inject the event.

Responsible Facilitator The responsible Facilitator indicates the Facilitator who is responsible for the event. This Facilitator is responsible for monitoring exercise play in response to each implementer and for entering the event implementer into exercise play.

Event Description The event description is a summarized version of a scenario action that has occurred, or that is being initiated, to cause an exercise player or organization to use established systems, execute or implement an established policy, or perform defined procedures during an exercise.

Expected Action The expected action describes results expected from the MSEL event. It is used by facilitators to assist in monitoring exercise progress as established in the MSEL. The expected action is especially valuable when tracking player actions. It is used by observers to determine the effectiveness of an event.

3.3 NESCOR Failure Scenario Tailoring

This section provides guidance on how to expand and tailor a NESCOR failure scenario for use in a cyber security TTX. Beginning with the high-level scenario below, it provides a template for creating a much more detailed failure scenario. This detailed scenario will be the basis for developing the MSEL.

3.3.1 NESCOR Failure Scenario DGM.11 – short version

Included below is the short version of the NESCOR failure scenario and is extracted from the *NESCOR Failure Scenarios and Impact and Analyses* document.

DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System

Description: A threat agent performs reconnaissance of utility communications, electrical infrastructure, and ancillary systems to identify critical feeders and electrical equipment. Threat agent gains access to selected elements of the utility DMS system - which includes all distribution automation systems and equipment in control rooms, substations, and on pole tops - via remote connections. After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, causing automated tripping of generation sources due to power and voltage fluctuations. A blackout of varying degree and potential equipment damage ensues. The remote connections might be established using a variety of methods or combination of methods. These include, but are not limited to, using a lost, stolen, or acquired utility linemen's laptop to access the DMS directly; compromising an active remote maintenance connection used for vendor DMS application maintenance; taking

advantage of an accidental bridged connection to the internet due to DMS misconfiguration; or subverting distribution control communications directly.

Relevant Vulnerabilities:

- *Physical access to mobile devices may enable logical access to business functions by unauthorized individuals,* specifically linemen and maintenance personnel company laptops used for remote connections,
- *System relies on credentials that are easy to obtain for access* to company computers,
- *Physical access may be obtained by unauthorized individuals* to proprietary utility documents and information,
- *Configuration changes are not verified for correctness* to prevent and detect human error in data center configuration (e.g., Ethernet cable plugged into wrong port),
- *System permits unauthorized changes* by allowing remote access for vendors to do application maintenance and troubleshooting,
- *System makes messages accessible to unauthorized individuals* in the distribution control communication channel,
- *System design limits opportunity for system recovery using reconfiguration* such as distribution networks that are more radial in nature than meshed, making network reconfiguration to restore power more difficult.

Impact:

- Loss of customer power,
- Disclosure of proprietary utility documents or information,
- Possible customer and utility equipment damage.

Potential Mitigations:

- *Require strong passwords* with complexity requirements for company devices and systems,
- *Train personnel* to protect company information and documents from unauthorized disclosure,
- *Define policy* on handling sensitive information. This includes substation one-line diagrams, equipment information, communication architectures, protection schemes, load profiles, etc.,

- *Train personnel* (operations and maintenance employees) to handle and protect company computing devices securely, incorporating two-factor authentication, requirements on storing devices, and reporting instructions in cases of loss or theft,
- *Create audit log* of all changes in HMI control actions,
- *Generate alerts* for all changes for all changes in HMI control actions,
- *Restrict remote access* of vendor connections (e.g., physically disconnect remote connections when not in use),
- *Encrypt communication paths* for distribution control communications,
- *Require 2-person rule* for to verify correct DMS configuration,
- *Implement configuration management* for configuration documents,
- *Confirm action* to modify data center physical configuration,
- *Isolate networks* (distribution control networks) by segmenting the distribution control network itself.

3.3.2 NESCOR Failure Scenario – Detailed Version

The next step in the process is to expand the short failure scenario and include additional information. The fields in the detailed scenario provide the foundation for developing the MSEL. As an example, DGM.11 is expanded below. The detailed scenario is extracted from the *NESCOR Analysis of Selected Electric Sector High Risk Failure Scenarios* document.

DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System

Describe Scenario

Description: A threat agent performs reconnaissance of utility communications, an electrical infrastructure, and ancillary systems to identify critical feeders and electrical equipment. The threat agent gains access to selected elements of the utility distribution management system (DMS) - that includes all distribution automation systems and equipment in control rooms, substations, and on pole tops - via remote connections. After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, possibly causing automated tripping of distribution level generation sources due to power and voltage fluctuations. A blackout of varying degree and potential equipment damage ensues. Remote connections to the DMS might be established using a variety of methods or combination of methods.

Assumptions:

- Remote connections for vendor access are tightly controlled (using a virtual private network (VPN)) and physically disconnected manually when not in use;

however, no formal procedure exists for disconnecting vendor access and unintentional sustained connections do occur

- DMS/supervisory control and data acquisition (SCADA) network is segregated from any corporate or public networks; however, DMS/SCADA is not completely air-gapped since a one-way connection exists to the corporate local area network (LAN) for data gathering purposes

- Some DMS/SCADA communications run over leased fiber cables and communication equipment that are shared with other entities. Communications are segregated either by devoting fiber strands to entities or through use of virtual local area networks (VLANs)

- Electrical infrastructure information (e.g., distribution system and substation one-line diagrams, equipment information, equipment location, etc.) and DMS/SCADA system documents (e.g., networking diagrams, communication equipment, communication protocols, etc.) are considered proprietary and protected from unauthorized disclosure; however, this information resides on corporate systems and networks that are more accessible from public networks

- Data logging is performed on DMS/SCADA systems, recording, at a minimum, the time and user's identity of all log-ins and control commands initiated (e.g., breaker close, connecting capacitor banks, configuration changes, etc.)

- Network intrusion detection is not present on the control system network; however, it is present on the corporate network

- Some utility linemen and communication personnel have laptops that permit connections to DMS/SCADA field equipment, communication devices (switches, head-ends, etc.), and DMS systems over the control system network (not from public networks)

- Company computers and systems require password authentication; however, complexity requirements are moderate and two factor authentication is not used

- Distribution management system communications are unencrypted and defense in depth practices have not been implemented

- The DMS/SCADA system is monitored 24/7 by dedicated control system personnel

- The control system network is flat

- Distribution system is largely radial, though some tie lines do exist at the end of select laterals

Variants of the scenario: Remote connections for reconnaissance and execution of this attack can be obtained by a number of methods.

- A disgruntled or socially engineered employee provides remote access to the DMS for the threat agent or directly carries out the attack

- Using a lost, stolen, or otherwise acquired utility linemen's laptop to access the DMS directly: requires company laptop configured for employee remote connections to DMS, username and password to unlock computer, username and password for access to the DMS (if different from the computer), access to physical communication channel (e.g., switch port, wireless connection, etc.)

- Compromising an active or unintentionally connected remote maintenance connection used for vendor DMS application maintenance: requires knowledge of when the remote vendor connection is active, capability to access the connection, credentials for log-in or some way to subvert credentials/connection

- Taking advantage of an accidental bridged connection to the internet due to DMS misconfiguration: requires knowledge of an accidental DMS internet connection (possibly through a port scan that was not detected by cybersecurity countermeasures), administrator privileges on the DMS (possibly requiring a stolen username and password or introduction of malware)

- Subverting distribution control communications directly: requires intimate knowledge of utility communication protocols, skilled and clever means of subversion (e.g., breaking encryption or authentication, access to physical communication medium (fiber, copper, wireless spectrum, etc.)

- Implanting, swapping, or otherwise covertly implementing removable media into the DMS system via a control system employee. The removable media contains malware to facilitate remote unauthorized DMS access. This requires sophisticated malware on removable media, detailed knowledge of the DMS

system, and clever means of getting removable media into the DMS system

- Supply chain attack on DGM equipment (i.e., relays, RTUs, servers, communication equipment, etc.) that installs rootkits on the devices to facilitate outside access to DGM network and equipment: requires physical access to devices during design, manufacturing, storage, or transportation, custom developed malware

- Subversion of TCP/IP layers on shared networking equipment (e.g., changing VLAN configurations on communication equipment) to gain access to DGM network: requires physical access to shared networking communication equipment, login credentials to obtain privileged access networking on equipment

Physical location for carrying out scenario:

- Physical access to the communication infrastructure will be required (e.g., fiber cables, copper land lines, wireless, etc.) for direct subversion of communications

- Access to manufacturing, commissioning, storage, or transportation facilities (e.g., factories, warehouses, etc.) will be required for supply chain attacks,

- Physical access to shared networking facilities (e.g., switching stations, area distribution nodes, etc.) is likely required for attack on shared communication infrastructure, though remote connections to shared equipment may be possible depending on the service provider

- Physical access to vendor communication or datacenter facilities may be required for subversion of vendor communications

- If the conditions are right, this attack could also be carried out remotely over the Internet

Threat agent(s) and objectives:

- Most likely threat agents, with the objective to create disorder:
    - Malicious criminals or criminal groups
    - Recreational criminals
    - Activist groups, to protest differences with utility
    - Terrorists
    - Nation States
- Malicious criminals, with the objective to camouflage or enable other criminal activity,
- Other threat agents:

- Economic criminals, for financial gain using extortion against a utility or paid by one of threat agents in the "most likely" list

Relevant vulnerabilities:
(Note: the vulnerabilities with italicized text are common vulnerabilities)

- *Physical access to mobile devices may enable logical access to business functions by unauthorized individuals*, specifically inadequate protection of linemen and maintenance personnel company laptops used for remote connections to DMS from loss, theft, or abuse, and from misuse when not under control of authorized individuals, These company laptops are used for remote connection to the DMS,
- Weak protection of specific control system access information
- *System relies on credentials that are easy to obtain for access* to company computers, for example, weak authentication on SCADA/DMS systems and equipment and weak passwords
- Weak passwords
- *Physical access may be obtained by unauthorized individuals* to proprietary utility documents and information such as proprietary infrastructure and SCADA/DMS information,
- Human error in control center configuration (e.g., Ethernet cable plugged into wrong port)
- *Configuration changes are not verified for correctness* to prevent and detect human error in data center configuration (e.g., Ethernet cable plugged into wrong port or violation of DGM security policies (e.g., plugging in USB drives in DMS computer))
- *System permits unauthorized changes* by allowing remote access for vendors to do application maintenance and troubleshooting, for example, remote access to DMS/SCADA for vendors to perform application maintenance and troubleshooting
- *System makes messages accessible to unauthorized individuals* in the distribution control communication channel, for example, distribution control communications sent in clear text
- Lack of defense in depth in DGM network
- *System design limits opportunity for system recovery using reconfiguration* such as distribution networks that are more radial in nature than meshed, making network reconfiguration to restore power more difficult

- Weak physical security of communication and personnel equipment, including access to shared communication hardware and facilities
- Little to no review of communication logs
- Little to no forensics capability in DGM network
- Sharing communication equipment and infrastructure with other entities

Relationship to NISTIR 7628 logical reference model functions: The Operations domain function 27-Distribution Management System is the suite of application software that supports electric system operations, including online three-phase unbalanced distribution power flow, switch management, and volt/VAR management. The DMS also communicates with the Operations domain function 29-SCADA, providing the threat agent with access to that software and commands for controlling compliant devices. These devices are represented as Distribution domain function 15-Distribution RTUs or IEDs.

Analyze Impact:

[a] Loss of customer power might spread to entire service area

- Depending on the sequence of the feeders tripped, timing of attack, severity of cascading effects (if any), and utility response, power loss can range from a select feeder supplying a town, portions of a suburb, a large city, or a large geographic area

[b] Possible customer and utility equipment damage

- Voltage sags and swells could damage customer electronic equipment
- Shifting electrical load might overload transformers and switchgear or blow fuses,
- Oscillatory behavior might damage distribution level generation

[c] Loss of customer or employee private information

- Utility employee names, home address, date of birth, vehicle registration plate number, email address, social security numbers, etc.

[d] Disclosure of the names of personnel, proprietary utility documents or information

- Precise location of critical feeders
- Manufacturer and model numbers of equipment
- Network architecture of DMS communications
- Installed operating systems and software, version numbers, patch levels
- Password requirements and cyber security countermeasures
- Policy and procedure documentation

The table below shows those general categories of impacts that are most relevant to this scenario, as they relate to the discussion above.

Table 3-1
Impact Categories for DGM.11

	Impact category	Text reference
1	Public safety concern	
2	Workforce safety concern	
3	Ecological Concern	
4	Financial Impact of Compromise on Utility (excluding #5)	[a]
5	Cost to return to normal operations	[a] [b]
6	Negative impact on generation capacity	
7	Negative impact on the energy market	
8	Negative impact on the bulk transmission system	
9	Negative impact on customer service	[a] [b]
10	Negative impact on billing functions	
11	Damage to goodwill toward utility	[a]
12	Immediate macro-economic damage	[a]
13	Long term economic damage	
14	Loss of privacy	[c]
15	Loss of sensitive business information	[d]

Detectability of occurrence:

- Detection of reconnaissance of DMS/SCADA and infrastructure information residing on corporate and control system networks may be possible given the presence of a network intrusion detection system (IDS) on the corporate side, the small landscape of the control system network, and data logging conducted on both; however, adversaries may conduct reconnaissance of electrical infrastructure by visually inspecting utility infrastructure (e.g., driving to substations and estimating line capacities, identifying equipment, etc.) which is more difficult to detect
    - Control systems that support the DMS are highly deterministic, so anything out of the ordinary would likely be detected and investigated

- A breaker trip, as well as the type of trip (e.g., manual trip, directional overcurrent trip, undervoltage trip, etc.) can usually be detected very quickly by control system personnel monitoring the DMS; however, the root cause of the trip (e.g., (fallen tree branch, equipment damage, intentional sabotage, etc.) takes more investigation, such as deploying trucks to survey feeders and equipment, connecting to relays to view logged events, etc.

- Software alterations and malware on DGM control equipment would be difficult to detect, especially those introduced in the supply chain

- In the case of reduced situational awareness, customers may notify utility of any loss of power due to an attack by telephone

- If privileged access to relays is obtained by adversary, logs from relays could be wiped or alerts to the control center may be disabled, making detectability more difficult

Recovery timeline: Typical recovery consists of:

- First 1-3 hours from disturbance (Preparation Actions)
    - Determination of information that is required to reconstruct the sequence of events, including attribution
    - Review standard restoration plans
    - Evaluate the post-disturbance system
    - Analyze the Customer Information System (CIS), monitor the DMS and dispatch maintenance workers to determine the cause and extent of the outage
    - Develop strategy for rebuilding the distribution network
    - Supply critical loads with the initial sources of power available

- 1 - 24 hours from disturbance (System Restoration)
    - Damaged components (if any) are repaired or replaced
    - Skeleton distribution paths are energized
    - Collect information and impound equipment as necessary

- Post Recovery
    - Review data logs on DMS, relays, phasor measurement units (PMUs), and communication equipment to determine:
        - sequence of events
        - how attacker gained access
        - mitigations to prevent attack from happening again

Analyze Factors that Influence Probability of Occurrence

Difficulty of conditions:

Condition numbers used here are shown in Figure 3-2 Figure 3-3, Figure 3-4, Figure 3-5, and Figure 3-5 below.

For *Condition (2) and Condition (11),* social engineering of an employee may be expensive and there is a risk of attribution if the attempt fails; however, social engineering of employees is not difficult.

For *Condition (7),* acquiring a company control laptop through theft may be trivial if the hardware is left unattended (e.g., being left in a company vehicle over lunch); however, if laptops and control equipment are left in locked boxes when unattended, acquisition is more difficult. Acquiring a company control laptop and credentials from a willing utility employee (or one that is amenable to coercion) can be easily accomplished through social engineering, bribery, blackmail, persuasion, or by force.

For *Condition (8),* knowing the exact moment that a vendor remote connection was inadvertently left connected will generally require substantial time and patience, depending on the frequency of remote vendor connections and the likelihood of control system personnel to forget to physically disconnect remote connections, but it is not difficult.

For *Condition (9),* scanning the utility network for accidental bridged connections to the Internet or corporate networks is, by itself, trivial; however, actually finding such a connection is exceptionally rare.

For *Condition (10),* connecting to the DMS by directly subverting the DMS communications is generally difficult, but can range in difficulty depending on the mix of communication mediums used. For example, subverting wired communications is more difficult than wireless communications, since access to the communication medium may be more difficult for wired communications.

For *Condition (11),* stealing or cracking employee credentials can be accomplished quickly and easily with the right password cracking equipment. If passwords are stored in databases as a hash, acquiring the hash values in the databases is moderately difficult.

For *Condition (12),* compromising an active remote vendor VPN connection for the purpose of a man-in-the-middle (MITM) attack is likely very difficult. Such an activity would require advanced capabilities and a high level of skill and knowledge.

For *Condition (4),* altering relay settings on its own is a very trivial task, given that relay software and user manuals are readily available by manufacturers, often at no cost. More difficult, is obtaining relay passwords (if they exist) that are not default passwords.

For *Condition (19),* spoofing telemetry data is moderately difficult, given the knowledge and skill required; however, many infrastructure measurement devices

can be easily altered by physical stimuli if physical access to the devices can be achieved.

No other Conditions in this scenario are difficult, though they are detectible using logs per the **Assumptions** information.

Potential for multiple occurrences: If this attack can be achieved once, it can be done multiple times; however, depending on the attack vector, lessons learned will make repeat occurrence on the same system less likely.

Likelihood relative to other scenarios:

- **A disgruntled or social-engineered employee** carrying out the attack is perhaps a utility's most vulnerable means of attack since the insider threat is difficult to defend against; however, this scenario is less likely to occur since logging and the immediate detection of breaker trips would limit the impact of the attack.

- **For a malicious criminal or terrorist**, the impact of a single attack is likely severe enough to warrant considerable interest. The higher level of skill and resources required for this attack is commensurate with established criminal or terrorist groups that have vast resources and highly skilled members. Additionally, the possibility of a large geographic area losing power might support a terrorist or criminal group agenda of causing significant financial harm.

- This attack might meet the goals of a **recreational criminal**. It is a challenge with a clear objective, and the attacker will remain anonymous; however, the difficulty of the attack and the high level of skill and resources required would generally limit their involvement.

Potential mitigations:

- *Require strong passwords* with complexity requirements or *require two-factor authentication* for company devices and systems (Condition 14, 16)
- *Require strong passwords* that are different for each relay (Condition 18)
- *Train personnel* (operations and maintenance employees) on handling and protecting company computing devices securely, requirements on storing devices, and reporting instructions in cases of loss, theft, and system recovery activities (Condition 7)
- *Restrict remote access* of vendor connections (e.g. physically disconnect remote connections when not in use or incorporating timed physical disconnects of remote connections) (Condition 8)

- *Restrict remote access* of vendors by installing patches and updates via physical media mailed by vendor, instead of allowing remote vendor access (Condition 16)
- *Encrypt* communication paths for distribution control communications (Conditions 8, 10, 11, 14, 16, 19)
- *Restrict physical access* to communication equipment in shared locations (Conditions 10, 19)
- *Require intrusion detection* on the DGM networks and hosts (Condition 16)
- *Minimize functions* on control system equipment by disabling all unused ports (Conditions 9, 10)
- *Check integrity* of firmware, applications, patches and updates (Condition 17)
- *Verify personnel* by performing thorough background checks on employees (Condition 1)
- In this failure scenario, social engineering can be used to convince an authorized individual of the need to take a specific DMS/SCADA action, or for a threat agent to obtain network access and DMS credentials (Conditions 2, 11, 13). General mitigations related to social engineering apply as shown in the common sub tree "*Threat Agent Uses Social Engineering.*"
- The following mitigations have not been mapped to a specific condition in the attack tree in this draft:
    - *Define policy* that requires prior notification and mutual consent of all participating for all modifications to be made on any shared communication devices *Require 2-person rule* to verify correct DMS configuration
    - *Isolate networks* (distribution control networks) by segmenting the distribution control network itself
    - Mitigations related to loss of proprietary business information during this occurrence of this scenario:
        - *Train personnel* to protect company information and documents from unauthorized disclosure
        - *Define policy* on handling sensitive information. This includes substation one-line diagrams, equipment information, communication architectures, protection schemes, load profiles, etc.

Organizations involved in scenario and recovery:

- Utility operations, utility field service or third party operations for sending disconnect command

- IT for closing off access to attacker

- Distribution Operations for rebalancing of system load

- Customer Service for interface with affected customers

References:

Source scenario(s): DGM.11 in [7].
Publications: None.

3.3.2.1 Attack Tree Diagrams

Modified attack tree diagrams were included for some of the detailed failure scenarios, including DGM.11. Following is a summary of the revisions to the standard attack tree format and structure. The graphical notation used for the attack trees is illustrated in Figure 3-1 and shows a modified annotated attack tree. Key aspects of this notation are:

- The tree is shown in each figure, with truncated branches represented by double lines around the numbered small hexagons. These branches may be shown on another figure.

- Each hexagon represents a condition in the sequence of conditions that make up a failure scenario. The leaves directly connected to and above a leaf represent the full conditions necessary for that lower leaf to occur. The conditions can be descriptions of several steps that must occur within a failure scenario.

- The tree is read from top to bottom, in terms of the sequence of conditions that occur. (This is a revision to the standard attack tree format – where the tree is followed from bottom to top. The objective was to provide a diagram that is easier to read.)

- A condition is labeled with the SOURCE that initiated that condition and the action (STIMULUS) that was initiated. A source is typically a human actor or a cyber component.

- The numbers that label each hexagon (condition) are ID's to enable a user to refer to specifics of the figure. They do not represent an ordering of condition. A double border indicates that the branch is truncated, and continues on another diagram.

- Connection of two conditions by a line means that the lower condition depends upon the higher condition.

- Connection by a dotted line means “OR”, that is, a lower condition can occur if either one OR the other of the connected upper conditions occurs. If all upper conditions are required for a lower condition to occur, a solid line is used, representing “AND.”

- At the bottom of the attack tree are two additional nodes – the first indicates what happens to the system after the failure scenario occurs (system response), represented with a rounded square, and the second describes the impact when this occurs, represented with an oval.

Common attack sub trees are a simplification technique that represents those subsets used in many attack trees, and is represented as a hexagon with double outlines as shown. Creating modular subsets simplifies the specific attack trees by allowing those common details to be documented in their own trees. The specific trees then instantiate a common attack sub tree with the pertinent context of how it is being referenced.

- The common attack sub tree has a common name, such as Threat Agent Obtains Legitimate Credentials, but also include the context, "for system or function”. The specific attack tree will then specify which system or function is referenced.

- The mitigation documented on the specific attack tree will state “See Common Sub Tree Threat Agent Obtains Legitimate Credentials for <system or function>”.

Several common attack sub trees are included in Section 3.4 of this document.

Figure 3-2 to Figure 3-5 show the modified attack tree diagrams for this scenario, DGM.11. These may be used in developing the MSEL.

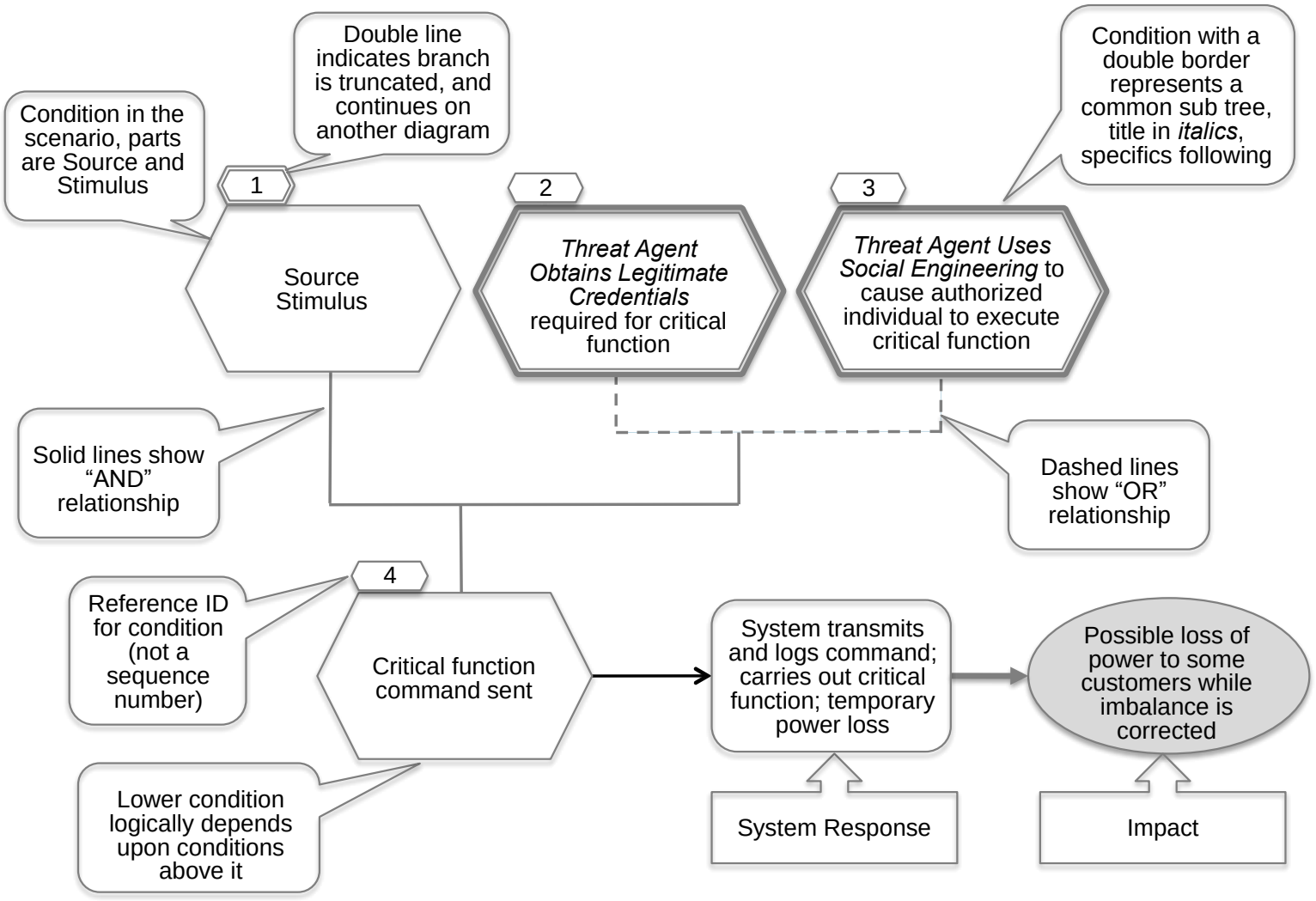


Figure 3-1
Graphical Notation for Annotated Attack Tree Format

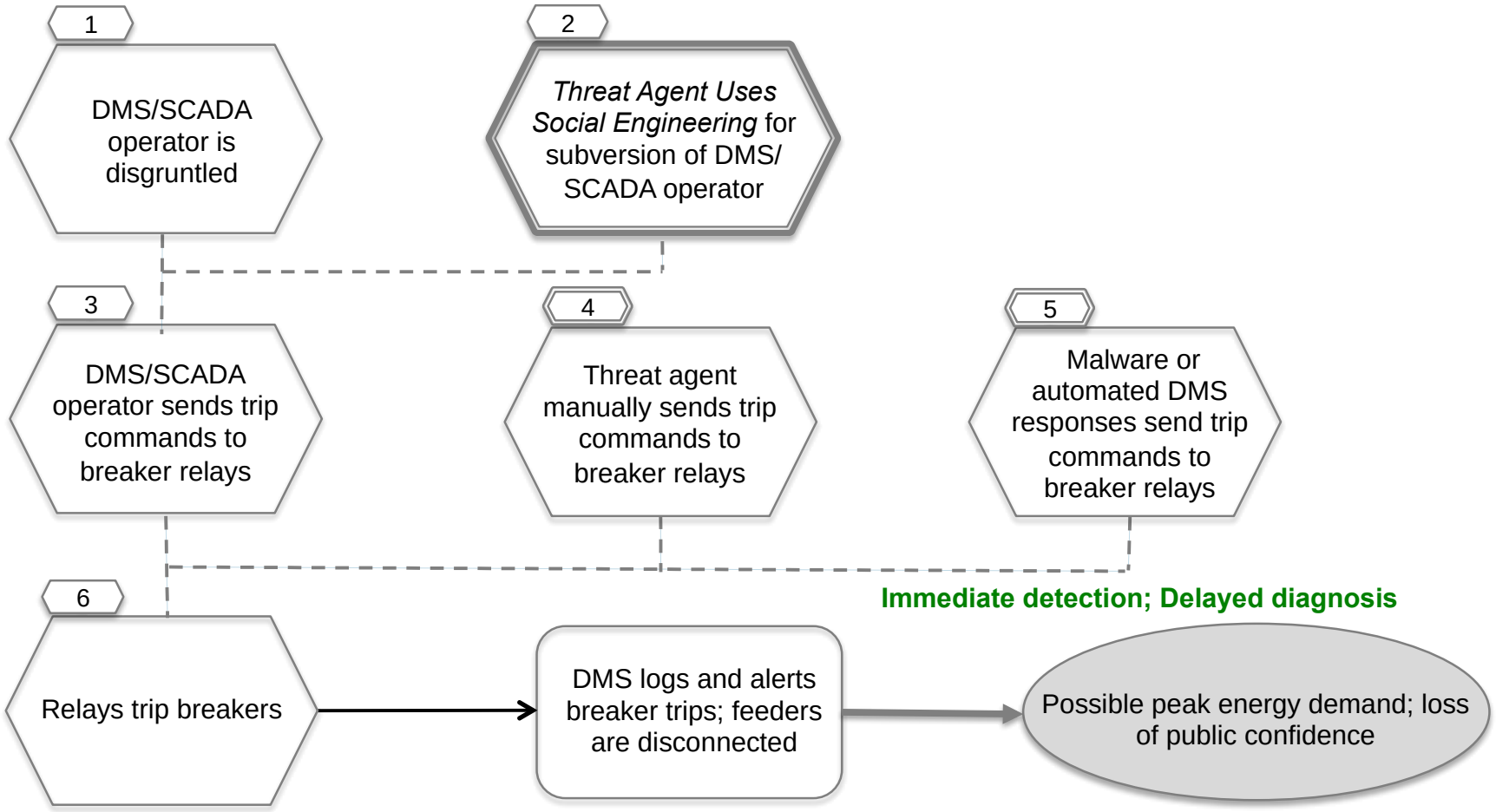


Figure 3-2
Threat Agent Triggers Blackout via Remote Access to Distribution System (1/4)

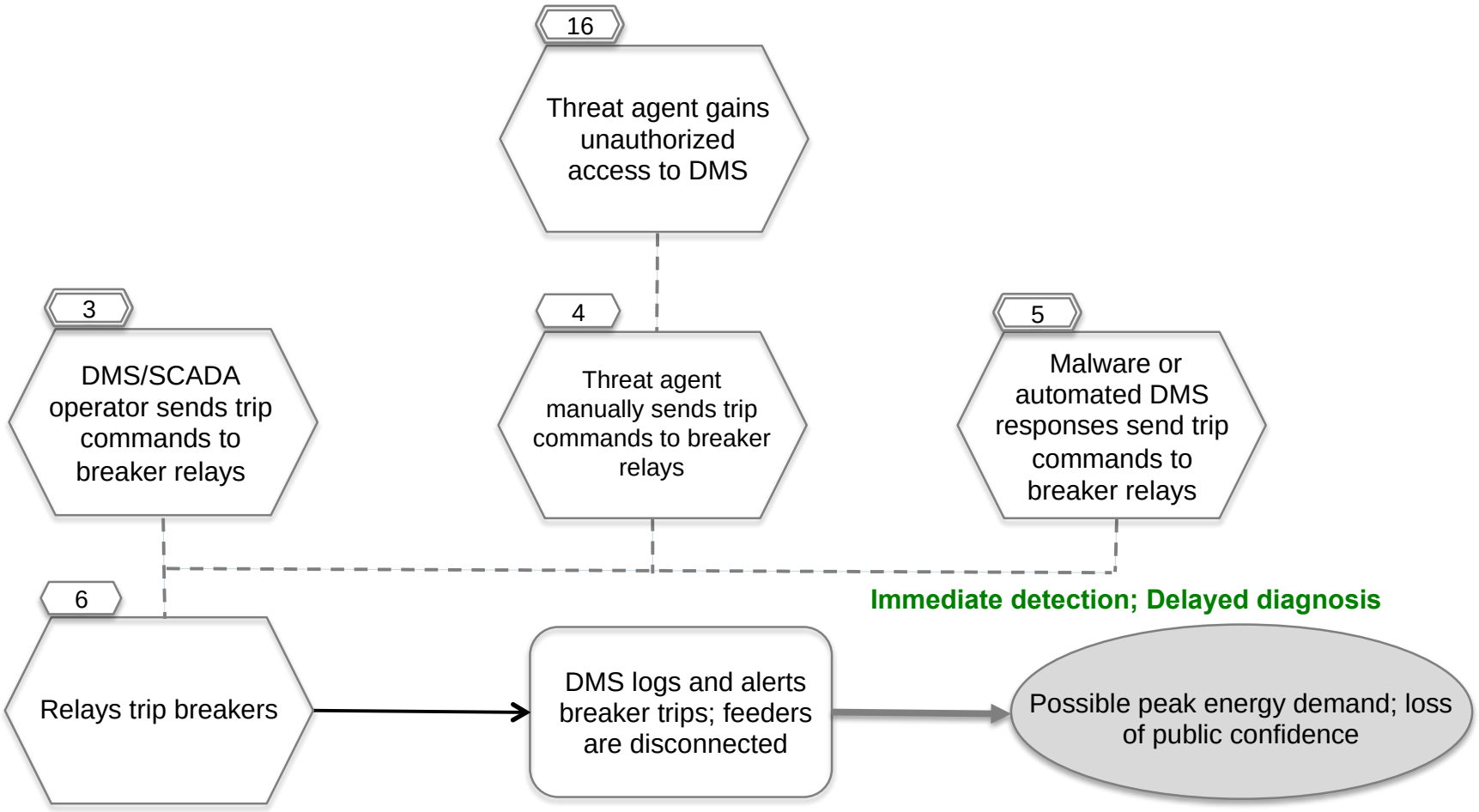


Figure 3-3
Threat Agent Triggers Blackout via Remote Access to Distribution System (2/4)

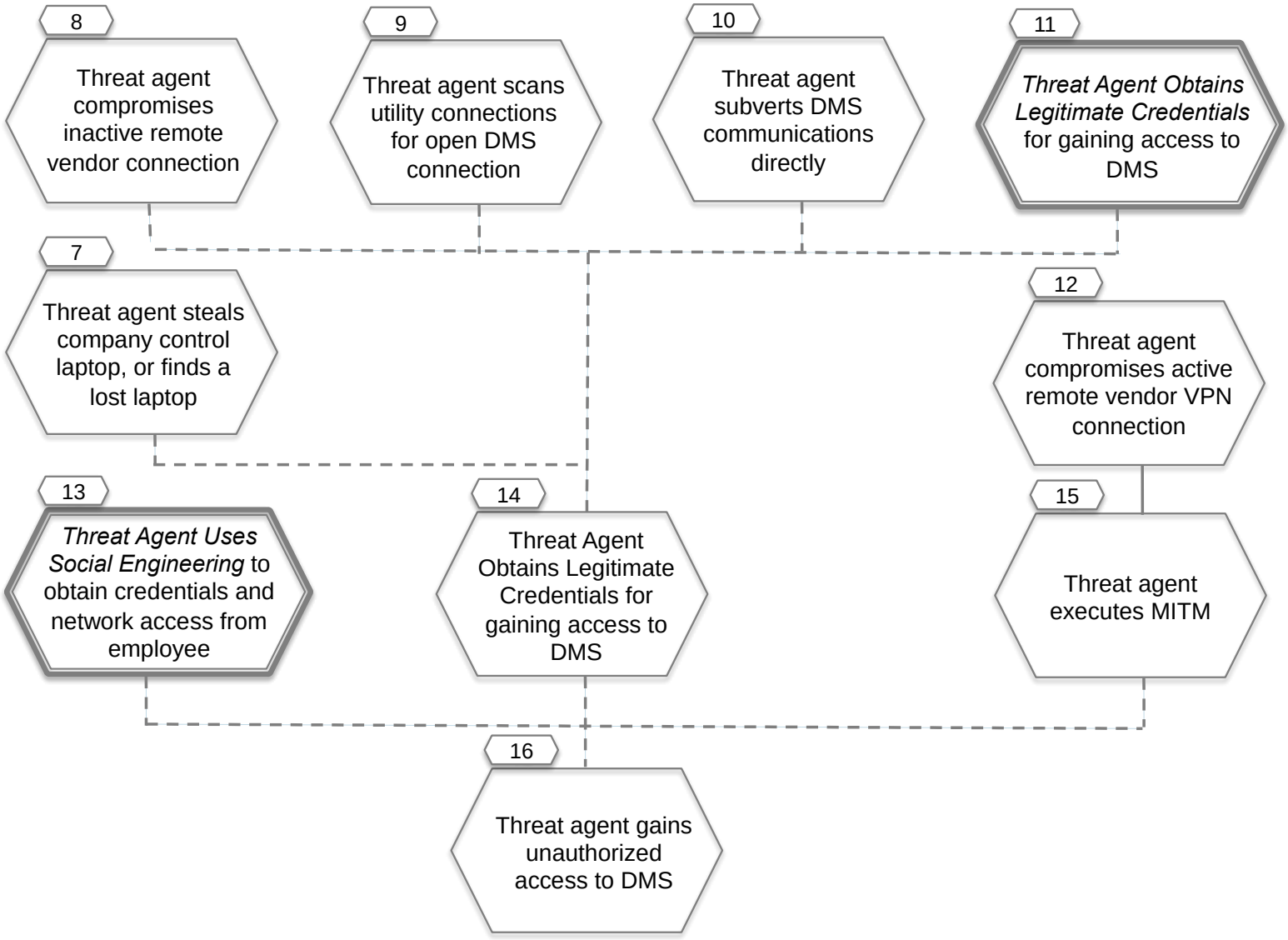


Figure 3-4
Threat Agent Triggers Blackout via Remote Access to Distribution System (3/4)

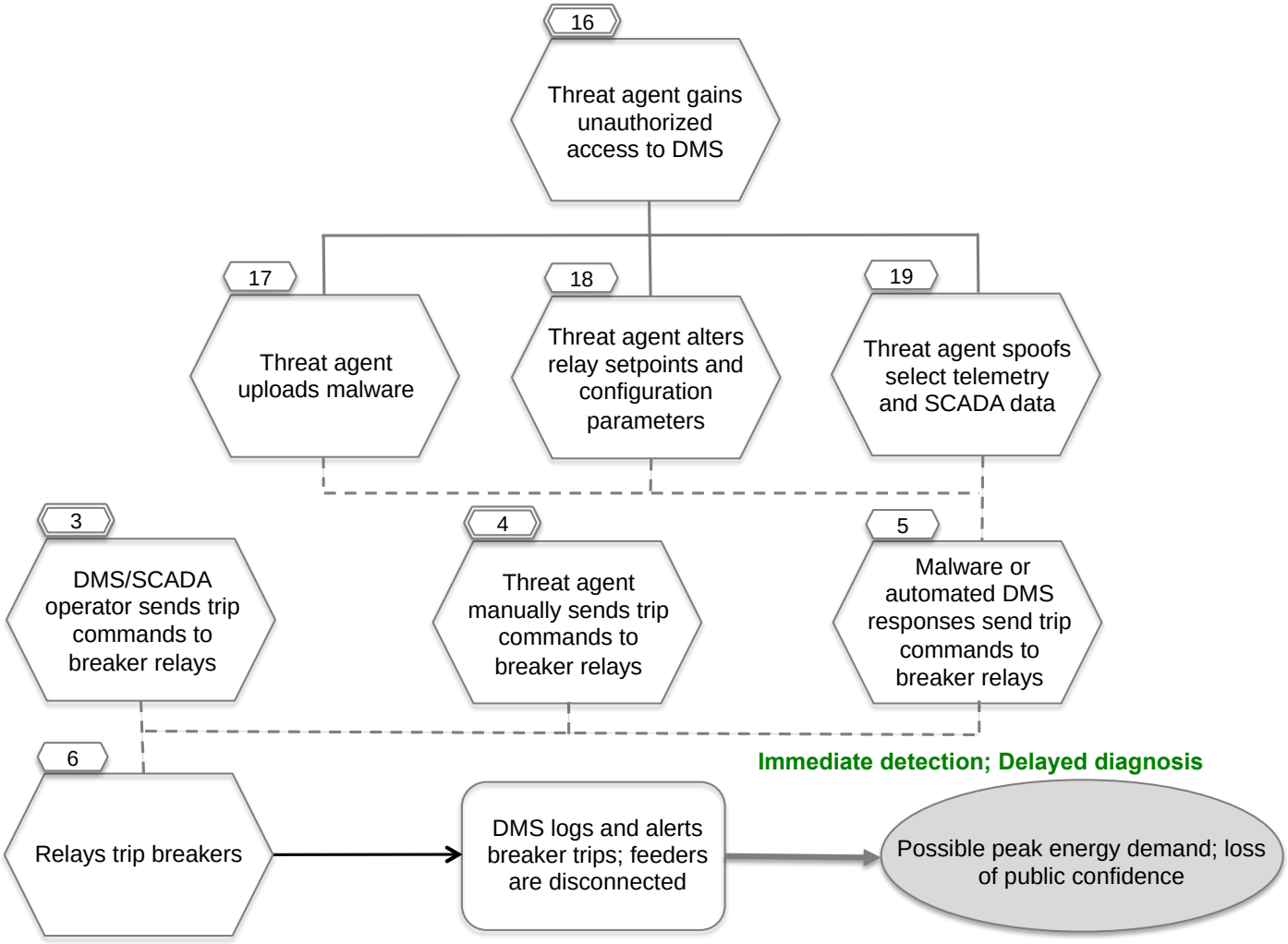


Figure 3-5
Threat Agent Triggers Blackout via Remote Access to Distribution System (4/4)

3.4 Common Attack Sub Trees

The following trees were identified while creating the NESCOR failure scenario attack trees, as a result of understanding where there were common branches that occur in several situations. They have been abstracted into trees that can be instantiated via the bracket '<>' notation, where the bracket is then filled in with appropriate detail when the common tree is used in a failure scenario tree.

The common attack sub trees may be extremely useful when developing the MSEL. They can be combined with the failure scenario as a starting point to the exercise or to add more complexity to the MSEL.

3.4.1 Threat Agent Gains Capability to Reconfigure Firewall

Common sub tree: Threat Agent Gains Capability to Reconfigure <Firewall>

Description: A threat agent gains the capability to change firewall rules on a specific firewall to permit types of traffic to flow through the firewall that will enable future attacks.

Assumptions

- Threat agent has access to a network to which the firewall has an interface

Mitigations

Conditions apply to the following figure(s).

- See common sub tree *Threat Agent Obtains Legitimate Credentials for <system or function>* (Condition 1)
- *Conduct penetration testing* to uncover firewall vulnerabilities (Condition 2)
- *Implement configuration management* in a strict manner for the firewall system (Condition 2)
- *Maintain patches* on firewall system (Condition 2)
- *Detect unauthorized access* through traffic monitoring, specifically to detect reconnaissance (Condition 2)
- *Require intrusion detection and prevention* (Condition 2)
- *Create audit log* of attempts to access firewall host (Condition 2)
- *Require authentication* for system and database access for firewall (Condition 2)
- *Restrict database access* on firewall to authorized applications and/or locally authenticated users (Condition 2)

- See common sub tree *Threat Agent Uses Social Engineering to <desired outcome>* (Condition 3)

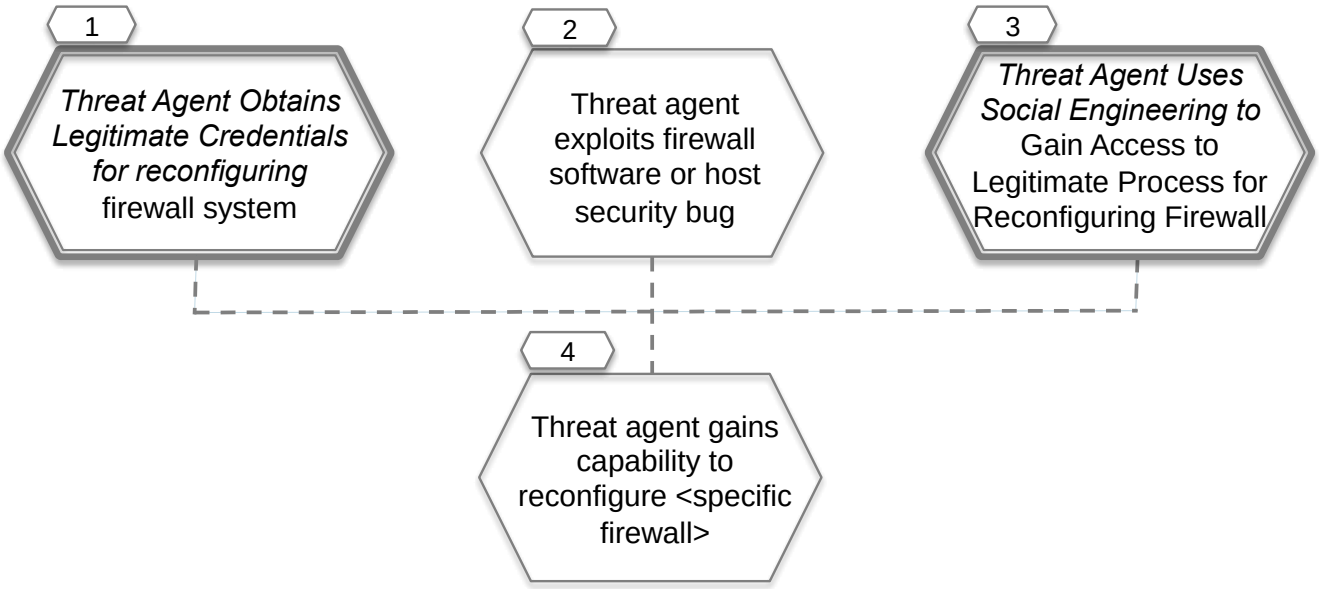


Figure 3-6
Threat Agent Gains Capability to Reconfigure Firewall

3.4.2 Threat Agent Blocks Wireless Communication Channel

Common sub tree: Threat Agent Blocks Wireless Communication Channel Connecting <x and y>

Description: The threat agent stops the flow of messages on a wireless communication channel connecting two entities, or slows it down to a point that it is essentially stopped.

Assumptions

- The backbone network for this wireless channel is wired, e.g., the Internet. Thus, wireless communication connecting <x and y>, in fact, consists of two wireless channels in the access networks: node x - wireless Access Point (AP) and AP – node y. Assuming these two channels are functionally same, this common tree considers the wireless channel between AP and a node. The terms ‘sender’ and ‘receiver’ refer to the entity that sends and receives the wireless signal, respectively, which may be an AP or a node.

Mitigations

Conditions apply to the following figure(s).

- *Restrict physical access* to AP and nodes (Condition 1)
- *Detect unusual patterns* on wireless channel; *Generate alarm* on detection (Condition 2)

- *Isolate network* for specific service; *Require spread-spectrum radio*; *Create audit logs* for network connectivity (Condition 3)
- *Create audit logs* for network connectivity; *Generate alarm* on network disconnectivity (Condition 4)
- *Generate alarm* on network disconnectivity (Condition 5)
- *Require acknowledgment* for message transmission; *Require redundancy* of communication channel to ensure message delivery (Condition 6)
- *Restrict physical access* to Sender; *Detect unusual patterns* on wireless channel; *Generate alarm* on detection (Condition 9)
- *Create audit logs* for transmission failure rate (Condition 11)
- See common sub tree *Threat Agent Gains Access to <network>* (Condition 12)
- *Detect unusual patterns* on association and authentication for wireless communication (Condition 13)
- *Generate alarm* on detection of abnormal association delay (Condition 14)
- See common sub tree *Threat Agent Obtains Legitimate Credentials for <system or function>* (Condition 15)
- *Restrict remote access*; *Detect unauthorized access*; *Require multi-factor authentication*; *Enforce least privilege* (Condition 16)
- *Generate alerts* on changes to configurations on AP; *Detect unauthorized configuration changes*; *Enforce restrictive firewall rules* (Condition 17)

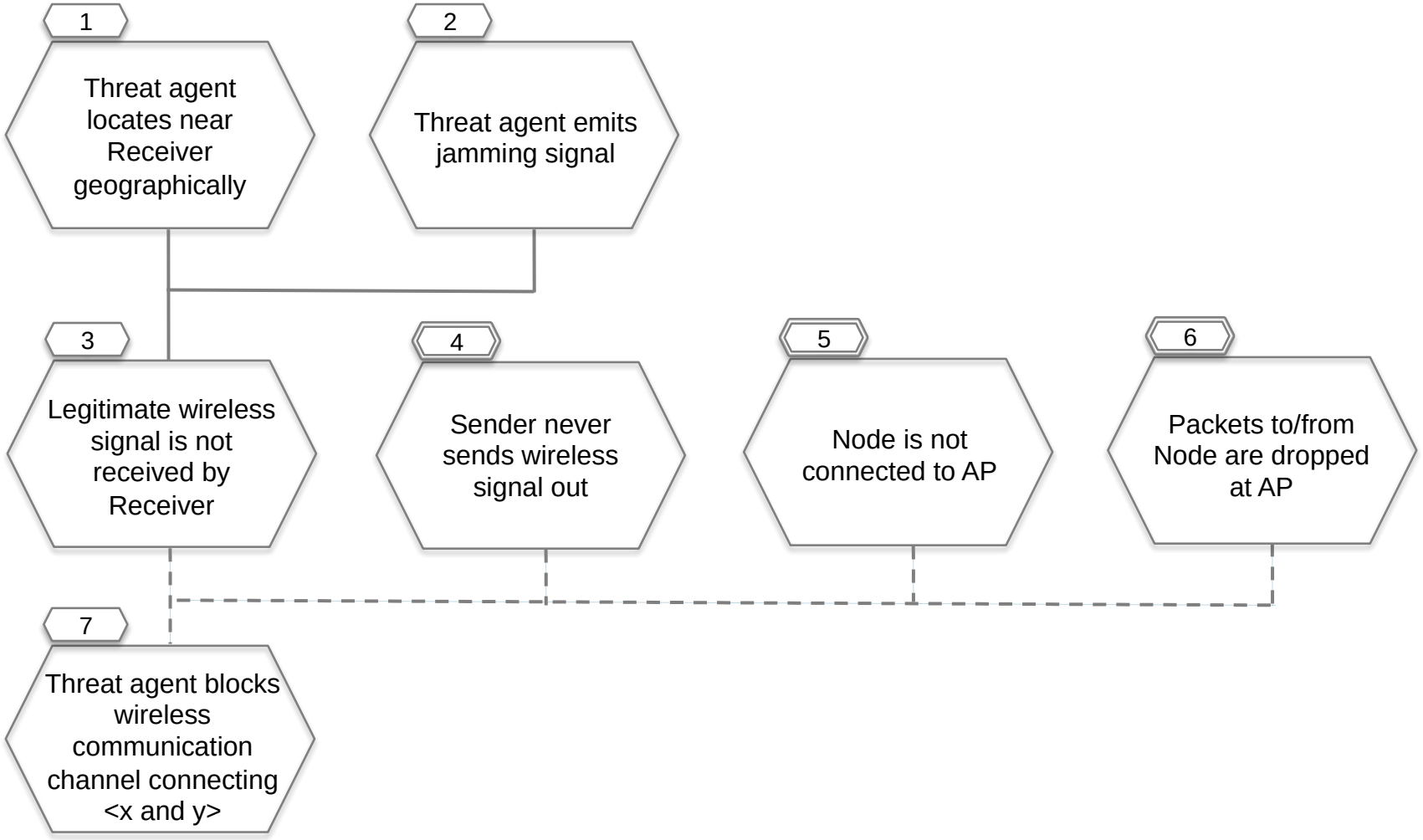


Figure 3-7
Threat Agent Blocks Wireless Communication Channel (1/4)

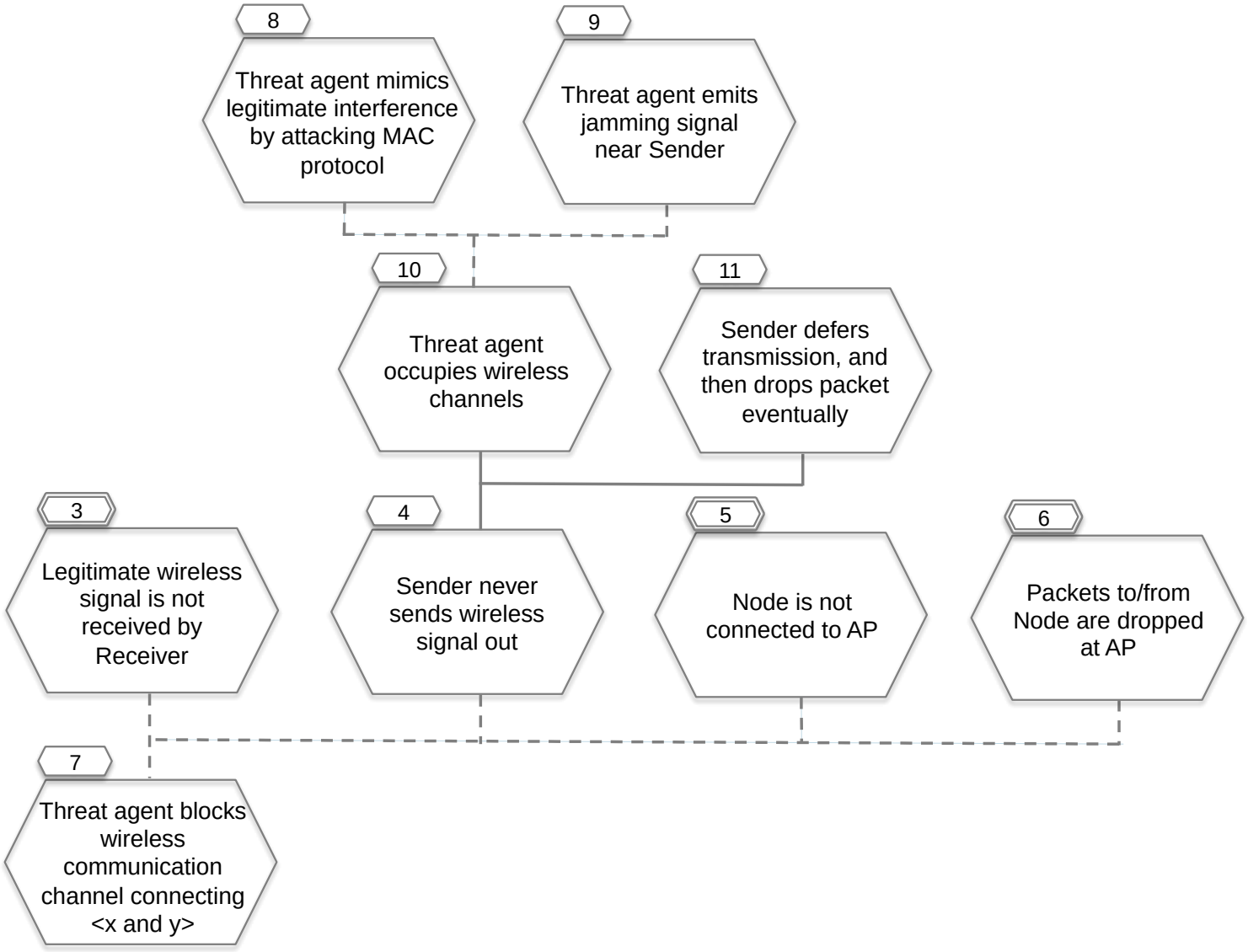


Figure 3-8
Threat Agent Blocks Wireless Communication Channel (2/4)

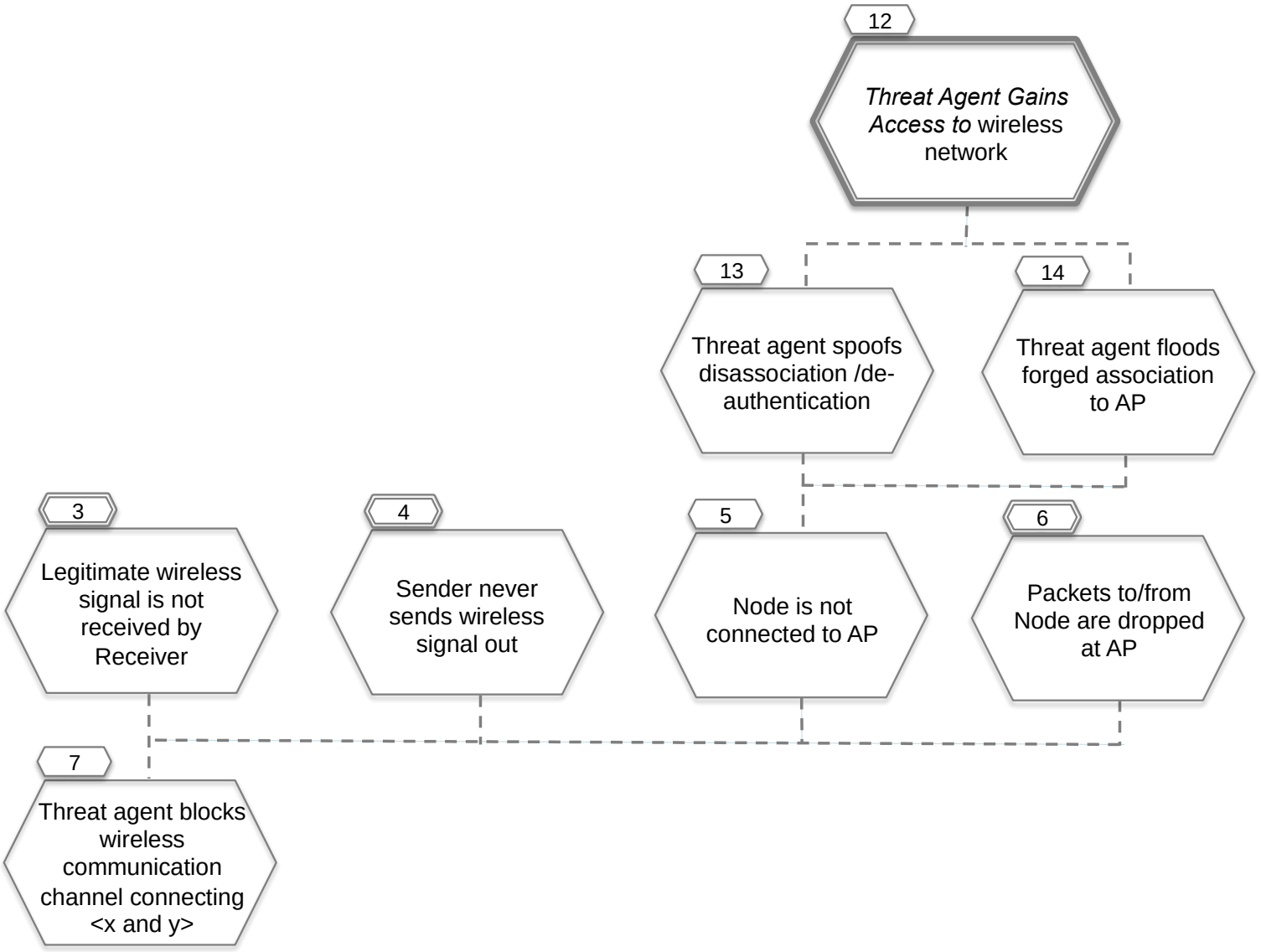


Figure 3-9
Threat Agent Blocks Wireless Communication Channel (3/4)

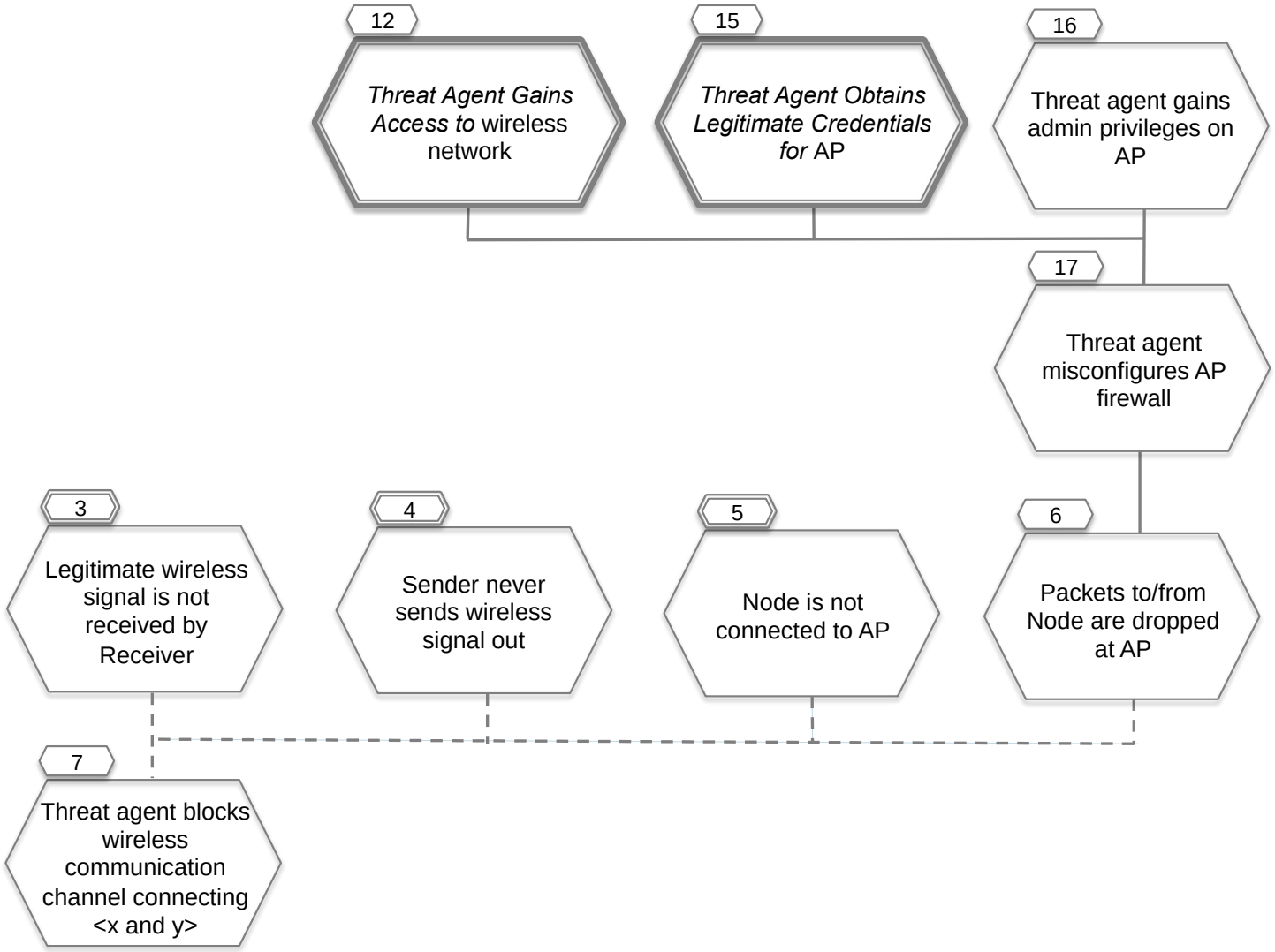


Figure 3-10
Threat Agent Blocks Wireless Communication Channel (4/4)

3.4.3 Authorized Employee Brings Malware into System or Network

Common sub tree: Authorized Employee Brings Malware into <system or network>

Description: An authorized employee uses the IT infrastructure to perform any action that results in the introduction of a particular piece of malware onto a specific network or a system.

Assumptions

- The network under discussion is protected by perimeter security tools (e.g., enterprise firewall), and communications within the local network is less restricted (e.g., no port number filtering and IP address filtering). Once a compromised device is connected to the local network, the malware may infect other systems in the network to compromise them. It is possible that a compromised device is under control a from threat agent remotely.

Mitigations

Conditions apply to the following figure(s).

- *Train personnel* regarding possible paths for infection to internal network (Conditions 1, 2, 3)
- *Maintain patches* on all systems; *Maintain anti-virus* on all systems (Conditions 1, 2, 3, 4)
- *Create policy* regarding connection of mobile devices and peripherals to the network; Test for malware before connecting mobile device or peripheral to local network (Conditions 1, 2)
- *Verify personnel* to find any previous actions against employers (Condition 4)
- *Require intrusion detection and prevention* (Condition 5)

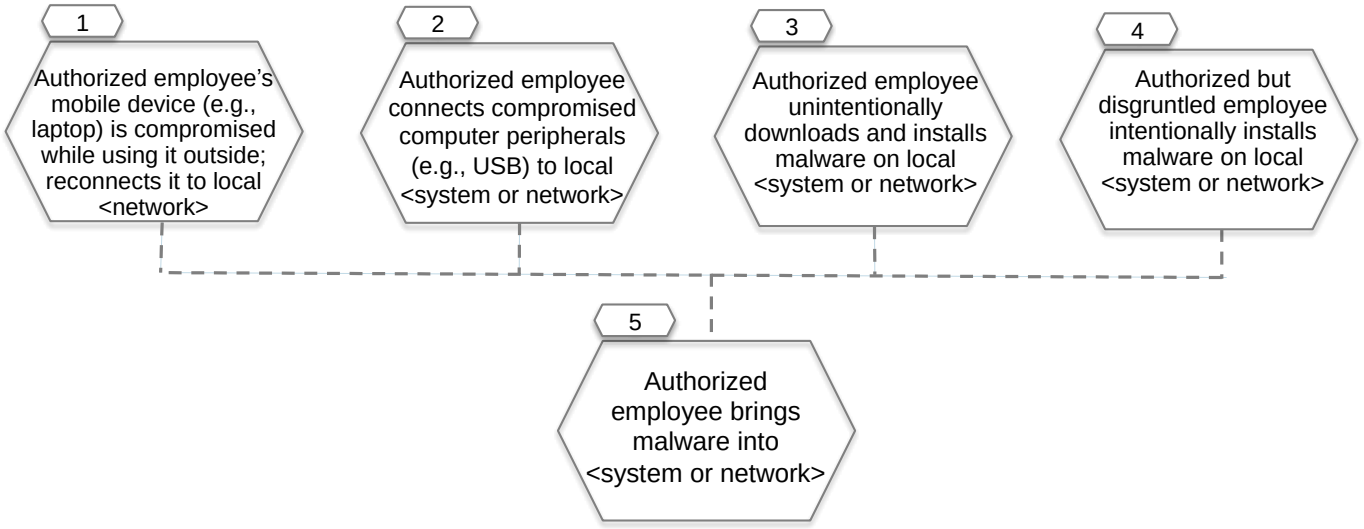


Figure 3-11
Authorized Employee Brings Malware into System or Network

3.4.4 Threat Agent Obtains Legitimate Credentials for System or Function

Common sub tree: Threat Agent Obtains Legitimate Credentials for <system or function>

Description: A threat agent may gain legitimate credentials for a system, or credentials that provide privileges to perform specific functions, in a number of ways. This includes finding them, stealing them, guessing them, or changing them. The threat agent may use social engineering techniques to carry out these methods. Each technology and implementation used for credentials is resistant to some methods and susceptible to others.

Assumptions

- Credentials used are either any static piece of data (referred to as a password) OR a physical object (such as a key card, referred to as a token). These are common forms of one-factor authentication. If two-factor authentication is used, such as a token with a PIN, the adversary must take more, similar steps to obtain all "factors" of the credentials.
- Other types of authentication exist, but are not in scope for this tree. They could be similarly analyzed

Mitigations

Conditions apply to the following figure(s).

- See common sub tree *Threat Agent Uses Social Engineering to obtain <desired information or capability>* (Condition 1)
- *Design for security* by using strong passwords (Condition 2)
- See common sub tree *Threat Agent Steals File* (Condition 3)

- *Design for security* by not recording passwords in log files (Condition 3)
- *Test for malware* on user workstations (Condition 4)
- *Design for security* by not sending passwords in the clear over the network (Condition 4)
- *Encrypt communication paths* on the network (Condition 4)
- *Protect against replay* on the network (Condition 4)
- *Design for security* by using strong security questions and protect answers (Condition 5)
- *Require multi-factor authentication* such as using a token with a PIN (Condition 6)
- *Define policy* regarding reporting and revocation of missing tokens (Condition 6)

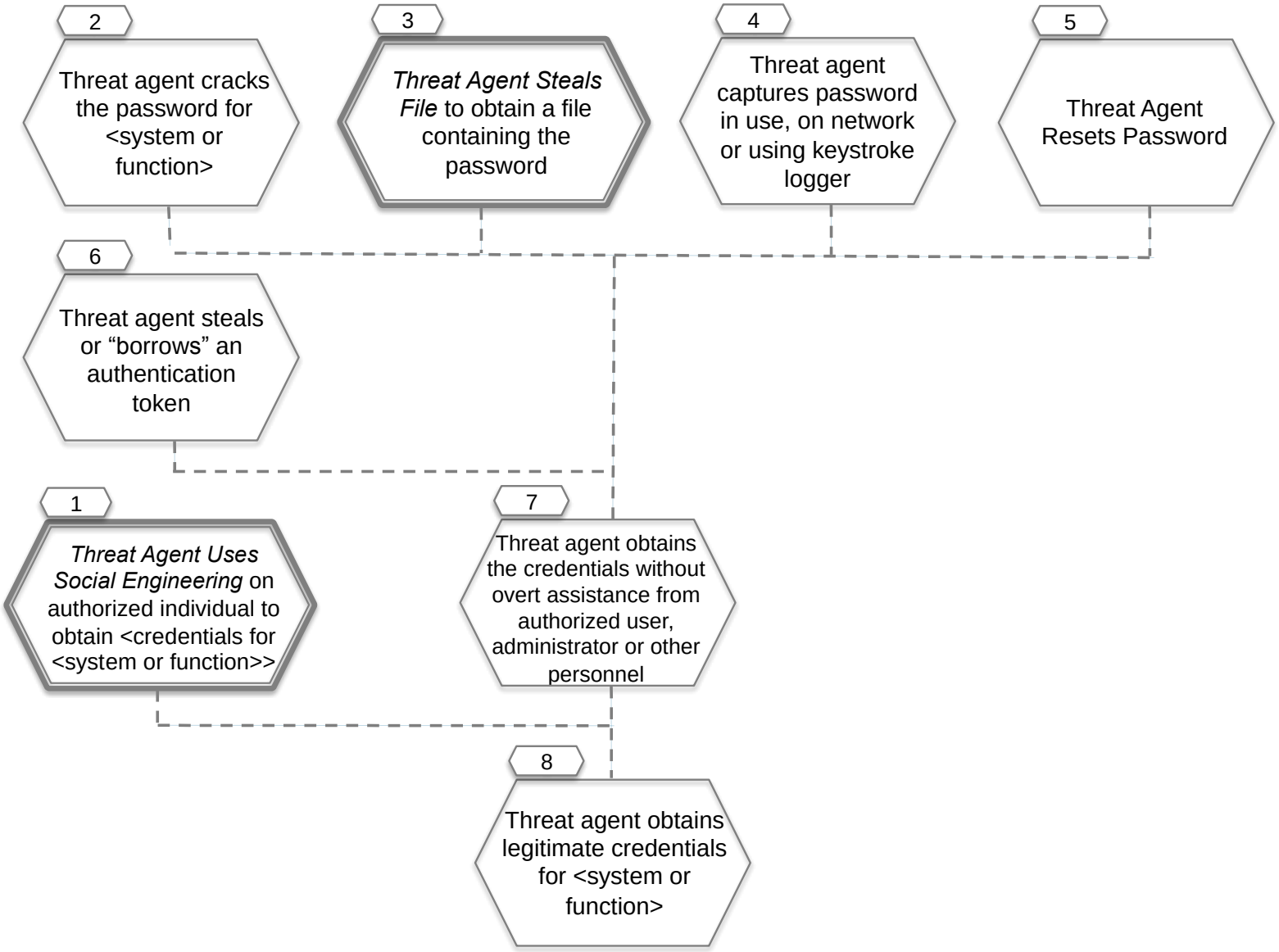


Figure 3-12
Threat Agent Obtains Legitimate Credentials for System or Function

3.4.5 Threat Agent Uses Social Engineering

Common sub tree: Threat Agent Uses Social Engineering to <desired outcome>

Description: A threat agent uses techniques of social engineering in order to persuade a victim to perform a desired action that results in an outcome that benefits the threat agent. Common examples of actions are to disclose particular information or to install/execute software that collects information or harms the victim's IT environment.
Notes:

- The attack tree provides an overview of the use of social engineering, there are many varieties
- More details and common examples may be found at: http://www.social-engineer.org/framework/Social_Engineering_Framework

Assumptions

- None currently identified

Mitigations

Conditions apply to the following figure(s).

- *Define policy* to minimize background internet disclosure, e.g., "do not make calendars public" (Condition 1)
- *Conduct penetration testing* periodically, posing as a threat agent (Conditions 1, 2, 3, 5, 6)
- *Define policy* to minimize leakage of physical artifacts (e.g., shredding, locked receptacle) (Condition 2)
- *Train personnel* that they are potentially targeted for these types of attacks and consequences for the organization can be serious. (Condition 5)
- *Train personnel* to report social engineering attacks (Condition 5)
- *Track social engineering attacks and warn personnel* (Condition 5)
- *Train personnel* including users and administrators in procedures to foil threat agent, e.g., "always call back to the number in the directory" and "always type in an authoritative web address" (Condition 6)
- *Detect abnormal behavior or functionality* via technical means, e.g., audit outgoing communications for sensitive data or unusual destinations (Condition 6)
- *Authenticate messages* automatically, e.g. require digital signatures, cryptography on email to authenticate trustworthy parties (Condition 6)

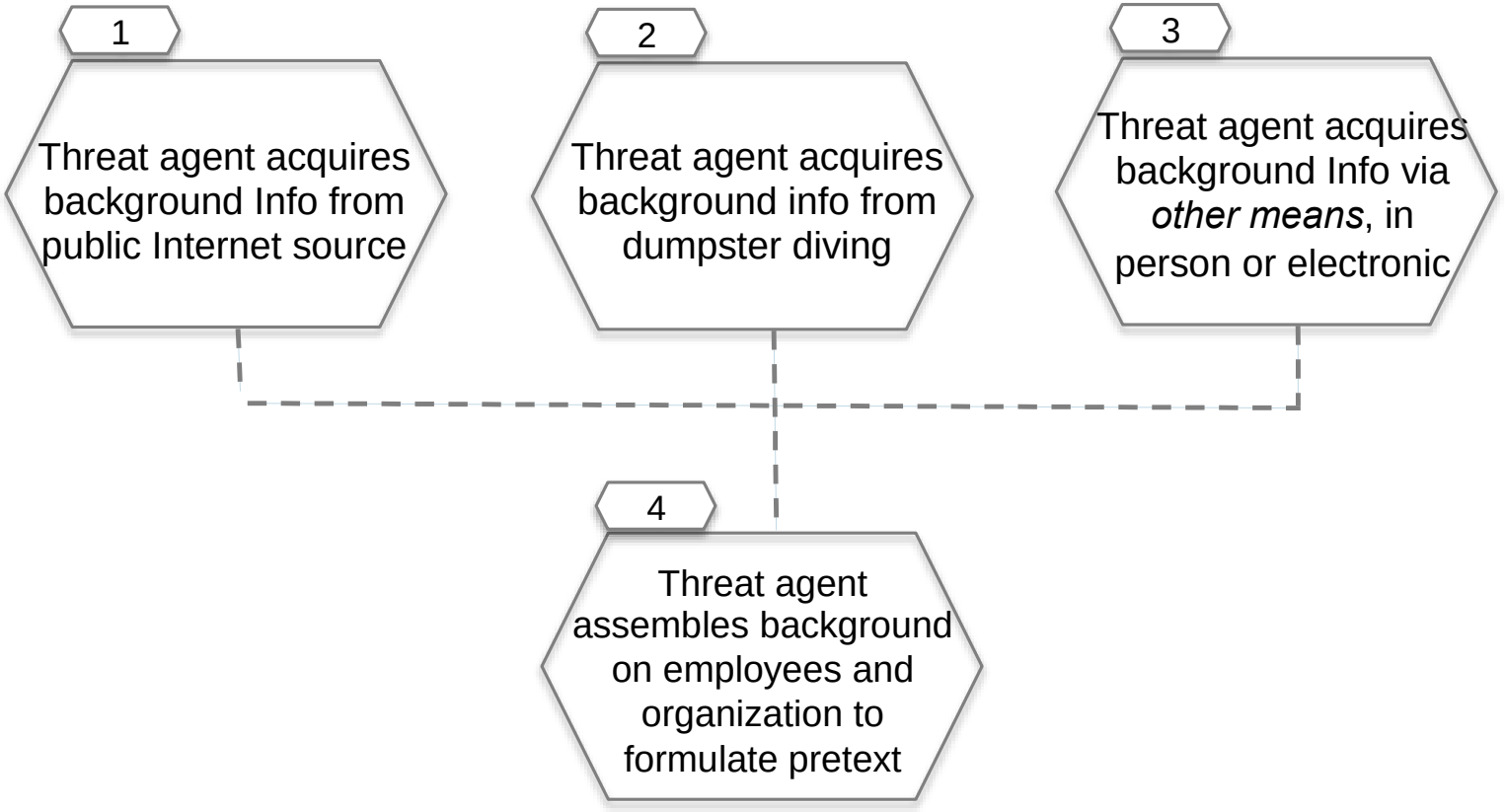
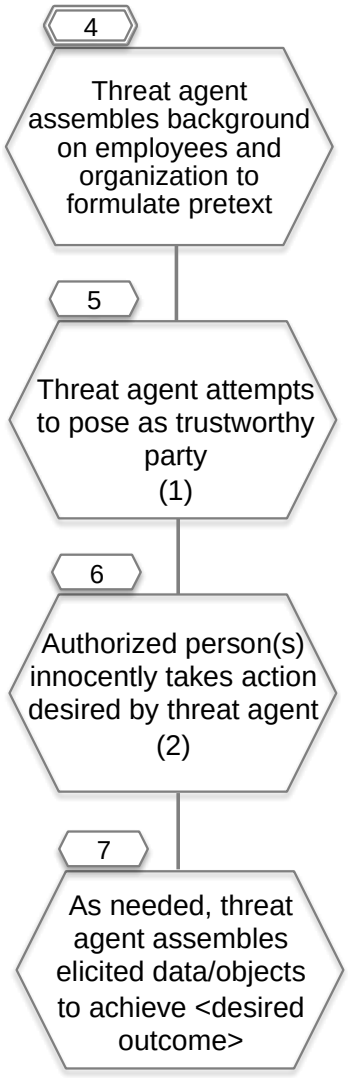


Figure 3-13
Threat Agent Uses Social Engineering (1/2)



(1) There are many effective techniques, all of which play on social/psychological aspects of trust. These can be pursued via any communication channel: in person (verbal/ non-verbal), on the phone, email, voice mail, fax, postal mail.

(2) This can be to release sensitive data (e.g., via voice, digital message or on a web site) or release an object (such as key card), and/ or to take some action that installs or executes a malicious program to gather data or performs other malicious actions.

Figure 3-14
Threat Agent Uses Social Engineering (2/2)

3.4.6 Threat Agent Finds Firewall Gap

Common sub tree: Threat agent finds firewall gap <specific firewall>

Description: An authorized employee either accidently or intentionally sets a firewall rule that allows an unnecessary and exploitable form of access to a network from another network.

Assumptions

- None currently identified

Mitigations

Conditions apply to the following figure(s).

- *Conduct penetration testing* to uncover firewall gaps, robust change/configuration management to protect entire system (Conditions 1, 2)
- *Verify all firewall changes* (Condition 2)
- *Require intrusion detection and prevention*, (Condition 2)
- *Require authentication* to network (Condition 3)
- *Authenticate users* for firewall application and database access, logging, and monitoring, (Condition 3)
- *Restrict database access* for the firewall to authorized applications and/or locally authenticated users (Condition 3)

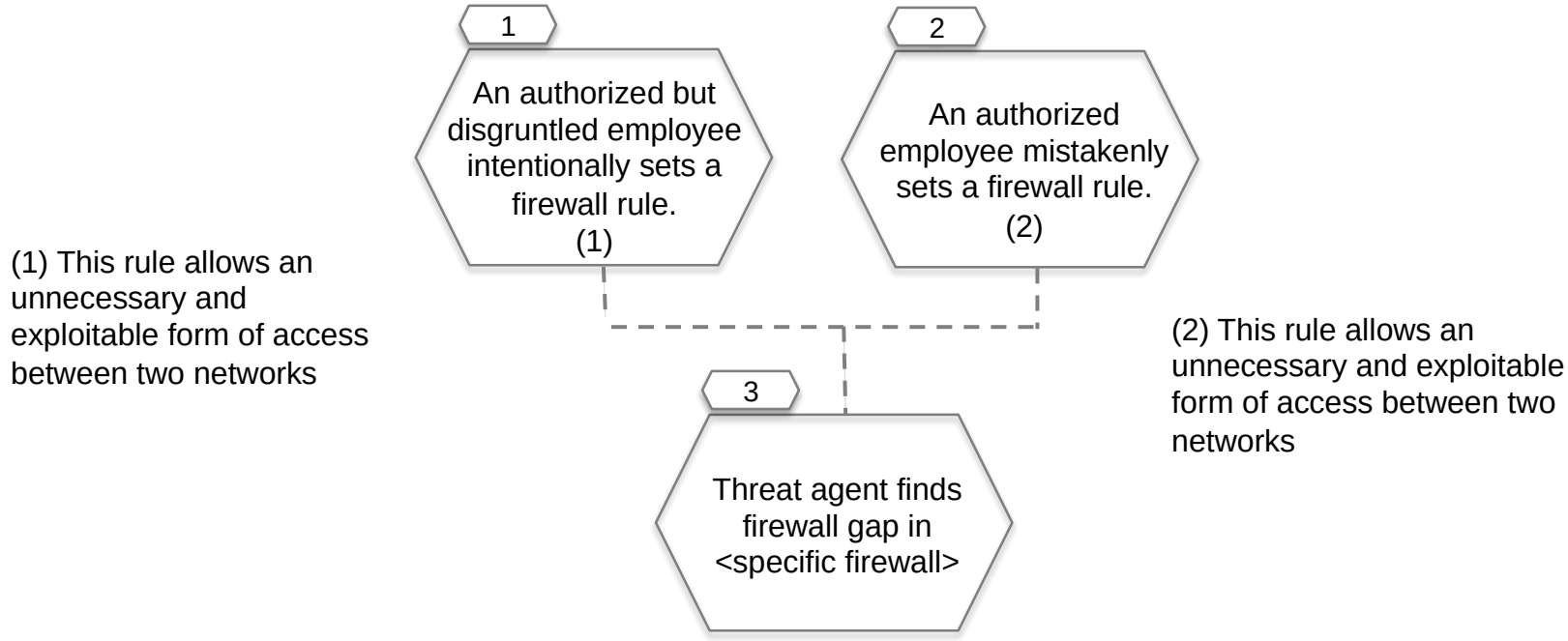


Figure 3-15
Threat Agent Finds Firewall Gap

3.4.7 Threat Agent Gains Access to Network

Common sub tree: Threat Agent Gains Access to <network>

Description: threat agent becomes capable of sending traffic within a network and attempting to communicate with its resident hosts.

Assumptions

- None currently identified

Mitigations

Conditions apply to the following figure(s).

- *Enforce least privilege* to limit individuals with privilege to the network and connected networks (Conditions 1, 2)
- *Isolate network* (Condition 2)
- *Enforce restrictive firewall rules* for access to network (Condition 3)
- *Design for security* by limiting connection points to networks that are widely accessible and by limiting number of hosts on same network (Condition 3)
- *Require authentication* to the network (Condition 3)
- *Enforce least privilege* for individuals with access to hosts on the network (Condition 4)
- *Detect unusual patterns* of usage on hosts and network (Condition 5)

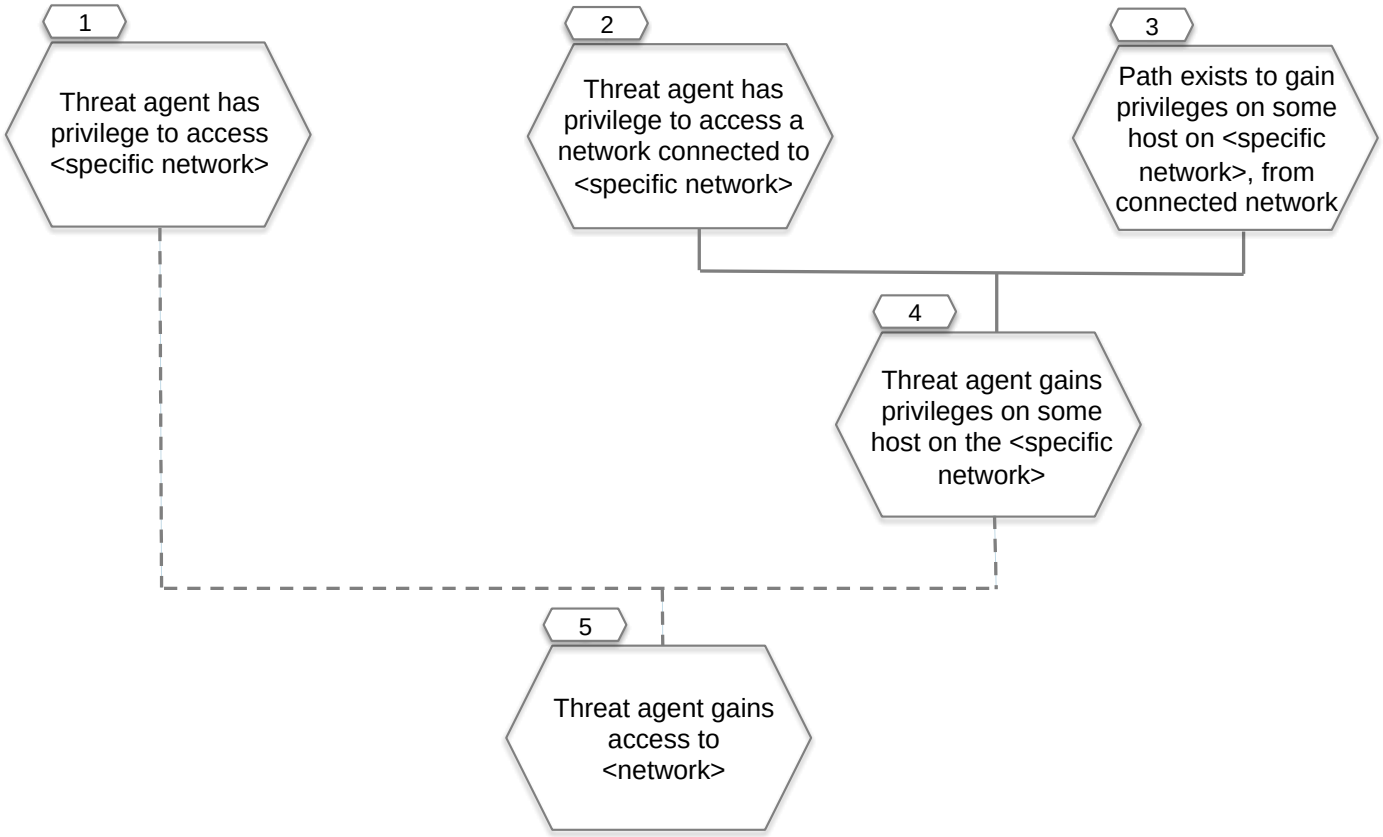


Figure 3-16
Threat Agent Gains Access to Network

3.5 Next Steps

Once the specific scenario set has been decided upon by the Planning Team, use the detailed scenario and knowledge of the organization-specific environment to prepare the messages and sequence for inclusion in the MSEL table below. There are several items that should be considered when developing the MSEL from the detailed scenario template:

- **Detailed injection time:** The events in the detailed scenario will need to be assigned specific and realistic times for both the event occurrence as well as injection into the exercise.
- **Recovery timeline:** For each event inject in the exercise, there is an expected action from the participants. The Recover Timeline field of the detailed scenario should provide high-level guidance for identifying the expected actions.
- **Single versus multiple locations:** If the exercise covers multiple sites, the Physical Location field in the detailed scenario may need to be expanded.

- **Organizations involved in scenario and recover:** As the exercise is being planned, it is critical to identify scenario planners from these organizations early in the process. This will result in a more realistic exercise and create greater buy in from the participants.

Table 3-2
MSEL Example

EXERCISE					
Event Num.	**Inject Time**	**From**	**To**	**Site**	**Facilitator/Observer notes**
1.1	10:30	Facilitator	All		Sent @ 10:21
Event Description: **Begin exercise play**			Expected Action(s): **Review scenario narrative for events to the present time. Begin actions based on plans & procedures relevant to the incident scenario narrative.**		

4
ACRONYMS

AMI	Advanced Metering Infrastructure
CIP	Critical Infrastructure Protection
CIS	Customer Information System
DER	Distributed Energy Resources
DGM	Distribution Grid Management
DMS	Distribution Management System
DR	Demand Response
DRAS	Demand Response Automation Server
EMS	Energy Management System
ET	Electric Transportation
EV	Electric Vehicle
EVSE	Electric Vehicle Service Equipment
FDEMS	Field DER Energy Management System
FEMA	Federal Emergency Management Agency
HSEEP	Homeland Security Exercise and Evaluation Program
IDS	Intrusion Detection System
IS	Independent Study
IT	Information Technology
LAN	Local Area Network
MSEL	Master Scenario Event List
NERC	North American Electric Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
OT	Operational Technology
PDC	Phasor Data Concentrator
PMU	Phasor Measurement Unit
SCADA	Supervisory Control and Data Acquisition
TTX	Tabletop Exercise
VLAN	Virtual Local Area Network

VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAMPAC	Wide Area Monitoring, Protection, and Control

5 REFERENCES

[1] *An Introduction to Exercises*. FEMA Emergency Management Institute (EMI) course IS-120a. http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-120.a

[2] *Exercise Evaluation and Improvement Planning*. FEMA EMI course IS-130. http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-130

[3] *Exercise Design*. FEMA EMI course IS-139. http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-139

[4] Homeland Security Exercise and Evaluation Program (HSEEP) templates. https://www.llis.dhs.gov/hseep/.

[5] *2011 NERC Grid Security Exercise After Action Report*. North American Electric Reliability Corporation (NERC). http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC_GridEx_AAR_16Mar2012_Final.pdf

[6] Grid Security Exercise (GridEx II) After-Action Report. NERC. http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20After%20Action%20Report.pdf

[7] *Electric Sector Failure Scenarios and Impact Analysis* (Version 2.0). National Electric Sector Cybersecurity Organization Resource (NESCOR). http://www.smartgrid.epri.com/doc/NESCOR%20failure%20scenarios%2006-30-14a.pdf

[8] *Analysis of Selected Electric Sector High Risk Failure* Scenarios. National Electric Sector Cybersecurity Organization Resource (NESCOR). http://www.smartgrid.epri.com/doc/nescor%20detailed%20failure%20scenarios%2009-13%20final.pdf

[9] *Attack Trees for Selected Electric Sector High Risk Failure Scenarios.* NESCOR. http://www.smartgrid.epri.com/doc/NESCOR%20Attack%20Trees%2009-13%20final.pdf

[10] *National Level Exercise 2012 Quick Look Report.* FEMA. https://www.llis.dhs.gov/sites/default/files/National%20Level%20Exercise%202012%20Quick%20Look%20Report.pdf

[11] *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability*. FEMA. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

[12] *Guide to Industrial Control Systems (ICS) Security.* NIST SP 800-82. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

[13] *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST SP 800-53. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[14] *Guidelines for Smart Grid Cyber Security*. NIST Interagency Report 7628. http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

[15] *An Overview of Issues in Testing Intrusion Detection Systems.* NIST Interagency Report 7007. http://csrc.nist.gov/publications/nistir/nistir-7007.pdf

[16] *Reliability Standards for the Bulk Electric Systems of North America*. North American Electric Reliability Corporation, 2014. http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf

[17] GridEx II overview presentation, GridSecCon 2013. Bill Lawrence, North American Electric Reliability Corporation, 2013. http://www.nerc.com/pa/CI/CIPOutreach/GridSecCon/2.08%20-%20GridEx%20II%20-%20Lawrence.pdf