Midwest Cyber Incident Coordination Scenario

FIRST MODULE

Current Situation

Six months ago (N-6 months)

State-sponsored actors successfully orchestrated a complex cyber and physical attack on a European nation's electrical grid. The incident resulted in a long-term power outage for two-thirds of the nation. The incident gained worldwide media attention—with discussion and images trending on social media for weeks.

Three months ago (N-3 months)

Electric Utilities in Minneapolis/St. Paul and Milwaukee detected breaches in their systems, removed the malware, and relayed the compromise to applicable authorities. In reaction to the discovery of that intrusion, national media released an in-depth investigative story revealing other previously unpublicized cyber intrusions and attempts to attack the United States' electrical grid by believed-to-be state-sponsored actors. The article took a leap in portraying a doomsday scenario involving an inevitable and imminent cyberattack on American intended to cause nationwide long-term disruption to critical infrastructure in the coming weeks. However, when no major physical impacts occurred, interest in the story waned after about a week.

This morning (N)

July 30th is a stormy summer morning in the Upper Midwest and there are scattered distribution outages throughout the area due to falling limbs and vehicular accidents that have taken down some poles. To complicate matters, in what is believed to be an isolated incident, an unknown number of individuals opened fire on a regional transmission substation hitting the main transformer, and backup transformer, destroying many of the facility's main components. To make matters worse, another key substation was down for planned maintenance, causing system operators to reroute power to another configuration. The multiple faults due to weather, the planned maintenance outage, and the attack has resulted in 1.5 million customers to lose power in the Twin Cities area in parts of the Upper Midwest. Local and state media outlets began reporting on the outage within two hours, prompting the story to start trending on social media.

As first responders and utility providers send resources to respond to the initial event outside St. Paul, utility providers notice a cascade of overloaded transmission lines failing in rapid

succession, seemingly unrelated to the initial substation attack, leaving about 80% of customers in Wisconsin and Minnesota without power – roughly 4.6 million customers including the 1.5 million customers in the Twin Cities affected earlier. This compounding factor complicates restoration and response efforts while amplifying confusion about the scope of the incident and the extent of cascading failures for critical infrastructure across the state. While utility providers are responding to the outage, rumors circulate that an attack has begun.

KEY ISSUES

- Public information coordination and management.
- Communication between responding government agencies and utility providers.
- Gathering and sharing of intelligence and information.
- Unknown incident scope and duration.
- Cascading impacts to other critical infrastructure.

DISCUSSION QUESTIONS

Based on the information provided, discuss the issues raised in Module 1. Identify any critical issues, decisions, requirements response actions, or questions that should be addressed at this time.

1. What are the utility general priorities for such a widespread power outage? Would they change in light of the European attack history and current public worry? If so, how and why?
2. What sources of intelligence and consequence assessment are in play to understand the scope of the incident?
3. How is information sharing managed for the gathering and sharing of intelligence? Are there any forums or mechanisms for near real-time information sharing? What might be the role of the Electricity ISAC, what would state intelligence fusion center be doing and what communication would be taking place between States Energy Assurance Coordinators and with the Department of Energy?
4. What specific actions is your agency taking to facilitate intelligence gathering and information sharing? What steps do you need or anticipate your response partners to be taking?
5. What information are utilities providing to your state EST-12 points of contact and/or the emergency management agency (EMA) at this time?
6. What information is your Governor seeking from utilities at this time and what information might the utilities feel would be important to be sharing with the Governor?

Second Module

The Next Day (N+24 Hours)

Information is coming out that believed-to-be state-sponsored hackers successfully gained control of 100 strategically located power generators servicing utility distributors across the

region, prior to the initial hack from three months ago that utilities believed had been patched. The hackers installed InfraRode—malware capable of directly controlling key circuit breakers in generator protection systems. The compromise has gone unnoticed until the adversary initiated their attack.

The damaged power grid has begun to overload causing electrical failures to cascade far beyond the immediately impacted area and into neighboring states. Phone and cell towers have switched to backup generation, internet and data is slow, and most gas stations cannot pump fuel. The virus has also affected the pipeline network, shutting down crude oil supplies to refineries. The Flint Hill Resources Pine Bend Refinery in Rosemount, MN, with a capacity of 310,000 barrels per day (b/d), the Andeavor St. Paul Park Refining at 98,515 b/d and the Husky Energy Superior Refinery in Superior, WI, at 38,000 b/d are idle due to either the loss of crude oil supply or the loss of power.[1] Hospitals may run out of fuel within 48 to 72 hours and other heavily equipped buildings would begin to operate on emergency power generation—slowly running out of fuel with every passing hour.

The public is anxious for an explanation. The confirmation of a cyberattack, and the nearly immediate worsening of conditions, builds the rumors into genuine fear that other regions may experience a situation similar to what they witnessed in Europe. Caught off guard and hungry for information, members of the public have been draining their mobile device batteries staving off boredom and looking for news on the outage. Cell towers in many locations are over loaded. There is already a growing sense of disorder as the public displays signs of unrest and dismay, fearing a long-term power outage lasting several weeks with substantial economic and social impacts.

KEY ISSUES

- Rising public fears and potential misinformation circulating on social media.
- Continuation and worsening of cascading effects prevalent in Module 1 increasingly affecting other critical infrastructure such as water systems and others.
- Public information coordination and management.
- Availability of cyber expertise.
- Public safety challenges with attack on critical communication method.

DISCUSSION QUESTIONS

1. What are your priorities and concerns now? Does the added intelligence of a cyber incident change response to the initial physical attack? What organizational plans are activated once a cyber incident is identified?
2. Are additional agencies notified in response to a cyber incident? If yes, which agencies?

[1] The production capacity for each refinery referenced in this scenario is the Atmospheric Crude Distillation Capacity (barrels per calendar day) as reported in the U.S. Energy Information Administration's Refinery Capacity Report and Data as of January 1, 2018, which was released on June 25, 2018 (https://www.eia.gov/petroleum/refinerycapacity/).

3. Does your agency have a mechanism for identifying cyber threats and responding to them?
4. Does public information coordination change with the new cyber element and/or other scenario update elements? How does the coordination change/continue?
5. For utility providers, does your organization have agreements or procedures to join the jurisdiction's Joint Information Center (JIC), if one is established?

Third Module

Two weeks later [or N+14 Days]

Power has been able to be restored to some isolated areas across the impacted region, but a majority of those affected remain without power. The physical damage to the generator systems caused by the InfraRode attack has proven to be too great to quickly repair, with critical system components needing to be replaced.

Your EMA has worked with partners to establish shelters and feeding for much of the affected population, but many have chosen to brave unsafe roadways to leave the area for the homes of friends and relatives in other currently unaffected cities and states until the power is restored. Your shelter workers are showing signs of stress and exhaustion after two weeks of sustained operations.

Schools have remained closed for the past two weeks; their buildings are uninhabitable without power. The schools that do have generator power have been turned into shelters. Some emergency generators have broken down due to the increasing long run time and even fuel for gasoline and diesel fueled generators is in short supply. Parents who have had difficulty finding reliable alternate care for their children have stayed home from work. Your region's largest retail employer has struggled to resume operations at its facilities in the area, leaving thousands of individuals without a source of income. Banks have not been operational in the region for two weeks. The lack of power has left railways, ports, and other crucial transportation supply chain modes unable to operate, halting operations.

KEY ISSUES

- Extended supply chain disruption.
- Escalating social impacts
- Large scale economic impact with business shut down and people out of work
- Challenges to provision of essential public services.
- Long-term staffing.
- Declining public confidence.

DISCUSSION QUESTIONS

Based on the information provided, participate in a discussion concerning the issues raised in Module 3. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

1. Within the Energy Sector, what are the potential cascading effects at this point? How can they be addressed and further mitigated?
2. What are the region's supply needs? How is the region obtaining these supplies considering any impacts to normal supply chain modes?
3. What is the availability to obtain, deploy, install and fuel generators to meet critical public safety needs and who at the state and federal level could support this effort?
4. How do agencies address public fear and lack of public confidence in response and recovery during a long-term power outage?