Preparing for a Large Scale Energy Sector Cyber Attack Case Study Packet

Keri Pearlson, Michael Sapienza and Sarah Chou

Working Paper CISL# 2020-04

December 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Preparing for a Large-Scale Energy Delivery Sector Cyber Attack*

Dr. Keri Pearlson, Massachusetts Institute of Technology
Michael Sapienza, Massachusetts Institute of Technology
Sarah Chou, Wellesley College

December 31, 2019

The case study, *Preparing for a Large-Scale Energy Delivery Sector Cyber Attack*, was written to illustrate potential gaps in the United States electricity sector's response to a major malware attack. This sector's complexity and interdependencies with other critical infrastructure sectors contribute to increasing the likelihood of such an attack. This case tells the story of a hypothetical scenario and the unique requirements that must be followed to respond to an attack at scale. This case was written to generate discussion about increasing the resilience of the energy ecosystem as a whole, and to identify appropriate participation from each member of the ecosystem. The hypothetical scenario is based on malware we have called Indestructor, but it is based on the real life incident known as CrashOverride that targeted Ukraine's power grid in late 2016.

This teaching tool includes a teaching note and a case study. To most effectively use this tool, the case study and study questions should be handed out to discussion participants to read prior to the discussion. The participants should be instructed to read the case and prepare their thoughts on the study questions. We have found that participants do best when they have at least one evening prior to the discussion to prepare.

The teaching note includes an overview of the case, study questions, a discussion flow, concluding remarks, outline of real malware incidents that has targeted the industrial control sector, and a second copy of the case study with numbered paragraphs for easy reference to the discussion flow. This teaching note is intended to give instructors one possible discussion, with questions to ask and sample answers to expect from the participants. However, an actual discussion may flow quite differently than this teaching note, and that is completely acceptable.

Comments should be sent to Dr. Keri Pearlson, kerip@mit.edu.

* This case and teaching note were written by Dr. Keri Pearlson, Michael Sapienza and Sarah Chou of MIT as a deliverable for the REMEDYS/REMAED project. This case was designed as a teaching tool for classroom discussion. These materials are based upon work supported by the Department of Energy under Award Number DE-OE0000780. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Preparing for a Large-Scale Energy Delivery Sector Cyber Attack*

December 4, 2019
Dr. Keri Pearlson
Michael Sapienza
Sarah Chou

Keeping the infrastructure of the country safe and secure is a non-negotiable need, but these same systems are constantly being targeted by cyber criminals' intent on disrupting operations. Though the United States electricity grid is considered to be safeguarded and reliable, no system is impermeable. While the grid regularly faces system failures and effects of natural disasters one threat that the United States electricity sector has yet to face is a large-scale cyber-attack that has catastrophic consequences. This is good news. But at the same time, cyber-attacks on all industries are becoming more frequent and the threat to the energy sector is no different. In the first three months of 2018, there was a 32 percent increase in cyber- attacks on US industries from the previous year.[1] Within the first six months of 2019, over 4 million data breaches occurred.[2]

While all cyber-attacks are of concern, the unique concerns for the electricity sector lie in the potential for a large-scale attack where multiple utility companies are hit simultaneously, or an attack on a critical utility company where there are compounding effects on others that cause a domino-like impact across the sector. The result of either of these types of attacks would be a crisis for the impacted utility, but in addition, there would potentially prolonged outages or other damages since there might be insufficient resources available to assist in recovery and returning to normal operations.

---

* This hypothetical case study was prepared by Wellesley student Sarah Chou, MIT student Michael Sapienza and MIT CAMS Executive Director Dr. Keri Pearlson for discussion and teaching. Any resemblance to any real organization is purely accidental. The authors would like to thank Hans Olsen, Mike Steinmetz and several other reviewers who asked to remain anonymous. Thank you to contributors Jess Smith from Pacific Northwest National Laboratory, Scott Baker, Jonathon Monken and Steve McElwee from PJM Interconnection, and Jake Schmitter from Electricity Information Sharing and Analysis Center (EISAC) and a number of other contributors who also asked to remain anonymous. This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

[1] https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/

[2] https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#48247dcebd54

Cyber threats increase due to the evolution of technology. Newer developments such as the internet of things (IoT), the cloud, smart grid tech, and IT/OT convergence are intended to increase efficiency and replace outdated systems, but they also introduce gateways for possible attacks. IoT specifically is quickly becoming more vulnerable, with nearly 3 billion cyber-attacks recorded as of September 2019.[3] When everything is connected to a network, even one that is 'air gapped' from the Internet, it becomes easier to bring down the whole system with a well-placed cyber-attack. Further, as innovations arrive at an increasing pace, it also becomes even more difficult for managers to adapt operations and response plans to keep pace with dynamic changes.

For many, it's not a matter of 'if a major attack will happen' but instead "when," and how to prepare for the "inevitable" as MIT Professor Stuart Madnick says.[4] Hackers are becoming smarter, constantly finding new ways to launch attacks, and defending against the unknown is difficult, if not impossible. Just follow the press, where many examples of countries such as Ukraine and Saudi Arabia faced cyber-attacks on industrial control systems in the energy delivery ecosystem. Should that happen in the U.S., the real effects of a cyber-attack on the energy delivery sector can range from momentary power outages to catastrophic physical infrastructure damage. The ramifications of a cyber-attack also reach further than the effects to the grid itself, threatening other critical infrastructure ecosystems such as the transportation industry, the water supply, and the economy as a whole.

Consider this hypothetical case study and the potential wide-reaching ramifications. On an average day in July where the electricity grid was functioning normally, areas of Massachusetts and Rhode Island began experiencing power outages. It was quickly identified that the areas affected belonged to two companies that serviced consumers across the two states: a transmission company Accelerated Grid and distribution company Light for All. Together, the two companies were responsible for power in parts of the Greater Boston Area and Providence, and most of southeast Massachusetts. The cyber-attack resulted in damage to a step-down substation run by Accelerated Grid, which ultimately affected the connected Light for All distribution lines. Within a few minutes, 1 million people were experiencing blackouts, and the number was growing. A short while later, states in the Midwest, namely in Illinois and Indiana also began experiencing power outages. Only one company, Connected Utilities, was affected in this region, though their transmission lines were connected to their own distribution substations responsible for bringing power to residents in cities such as Bloomington and Effington. Around 150,000 people lost power in that region. (Figure 1)

[3] https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#247336685892
[4] https://hbr.org/2017/05/preparing-for-the-cyberattack-that-will-knock-out-u-s-power-grids

The companies initially believed the outages were a result of a system failure and began the normal detect and recover processes. It took five hours to diagnose the cyber-attack. Given that cyber-attacks are not constrained by geographical boundaries, the threat actors were able to target these two completely different highly-populated geographical areas without much effort.

Prior to this, neither the southern Midwest nor eastern Massachusetts and Rhode Island had ever experienced major disturbances to the grid, since like most utility companies, their local suppliers had taken a proactive role to ensuring that the grid was as strong and stable as possible. The companies contracted with vendors to make sure their software was up to date and they had already begun to phase out old and vulnerable equipment. In addition, they also had strong, consistent network monitoring and cybersecurity processes. In the event of an anomaly in their network, retainers with third-party cybersecurity platform vendors kicked in. The companies involved believed they were protected against an event like this up until now.

Preparation

All three companies had response plans that outlined responsibilities for real time operators to restore power. The employees also went through training that taught them what to do during an emergency situation. As transmission companies, Accelerated Grid and Connected Utilities were subject to the NERC CIP standards, which describe standards for transmission companies that include aspects of required training, incident reporting, and vulnerability assessments, among other things. Part of the standards requires companies to train employees on items such as identification and recovery of cyber incidents, all intended to prepare for an attack on critical infrastructure.[5] Because CIP standards do not specifically state the required preparation metrics, leaders at the companies felt they were prepared for a cyberattack, but in reality, they had never performed a physical response drill. Their preparation had been table top exercises or communications exercises which did not simulate real time effects of a cyberattack, such as loss of communications, limited access to in-house expertise, or response to physical damage. In addition, they had not practiced recovery with their vendors, and while they knew who to call they did not have additional plans in place should their standard vendors be unavailable or unable to assist. On the other hand, Light for All as a distribution company falls under the jurisdiction of state governments, which focuses on ensuring that the state offers aid to companies in need both in its resilience plans and response efforts. However, all states have different standards and there is inconsistency in the way they are organized and presented.

[5] https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-004-6&title=Cyber%20Security%20-%20Personnel%20&%20Training&jurisdiction=null

BACKGROUND ON THE UTILITY COMPANIES

Accelerated Grid

Like most utility companies, Accelerated Grid had in-house teams responsible for spearheading response efforts when emergencies occur. On-site operators were familiar with all aspects of their substations and received training on how to manually fix all parts of the system when something failed. They also had a team of industrial control experts to handle damage or disruptions to substations. Accelerated Grid had recently hired two cyber experts that specialized in diagnosing and analyzing cyber problems to find the root cause. As a larger company responsible for supplying power to parts of major cities including Boston and Providence, Accelerated Grid also had sophisticated network monitoring capabilities, which allowed them to recognize issues relating to server connections, end point failures and other potential network issues. The company also had trained their teams with simulated cyber-attacks on their system, to ensure that the experts were familiar with the available resources.

One initiative in the cyber plans for Accelerated Grid was the Cyber Mutual Assistance (CMA) program, the Electricity Subsector Coordinating Council (ESCC)'s program dedicated to aid in the event of a cyber emergency.[6] Accelerated Grid expected CMA to send personnel and equipment in the event of a cyber emergency, as their network of experts offered specialized knowledge on these critical issues that Accelerated Grid employees did not have. However, CMA faced similar limitations in resource availability as other vendors. Transportation and quantity of energy to affected utilities was available but in a limited manner and for a short time. Long term or widely impacted geographical attacks would severely tax the CMA support. CMA is also limited due to the nature of cyber-attacks; lack of geographical boundaries leaves nearly every company vulnerable to the threat, and many may not voluntarily lend their resources in case they may get hacked in the near future. They are supposed to seek CMA help when their in-house cyber employees have exhausted their knowledge in the problem at hand, though there is no objective time in which they should call.

As a larger company, Accelerated Grid maintained a direct relationship with the Department of Homeland Security (DHS). The relationship included an agreement that in the event of a situation where it was needed, DHS would send a fly away team to aid in restoring power. In their plan, employees at Accelerated Grid worked with the National Cybersecurity & Communications Integration Center (NCCIC) and the Director of the Hunt and Incident Response Team (HIRT) in the event that all other internal operations to restore power failed, or if the situation became too severe for the in-house teams to handle.

---

[6] http://www.electricitysubsector.org/-/media/Files/ESCC/Documents/CMA/Cyber-Mutual-Assistance-Program-One-Pager.ashx?la=en&hash=785A8D66D3F21234FF0584FBA026A240FE123130

Light for All

Though Light for All's distribution system is connected to Accelerated Grid, the two were separate entities and did not share resources when it came to response mechanisms. Light for All's response plan however, similarly included on-site operator training on repairs to the substation and specific parts of the transformer systems. However, their response plans stated that they needed to call Stronger for You, their industrial control systems vendor, for help with repairs in the event of a blackout. Light for All did not have any in-house cyber employees. Instead they had a relationship with a CV1, a cyber vendor who was on contract to identify, respond and assist in recovery from a cyber-attack. However, their plans did not clearly state when the employees should call the cyber vendor for help. Managers used CV1 primarily for issues with data breaches or hacks in their corporate office. While their contract had provisions for assistance in the event of an attack on their industrial control systems, CV1 expertise in industrial control systems was limited. CV1's Boston office had 10 employees on call to assist customers with cyber-attacks, including Light for All.

Connected Utilities

Connected Utilities' response plan for emergencies relied on external help, given the limited amount of resources and personnel trained to handle blackouts and potential cyber- attacks. Like the other two companies, operators at Connected Utilities had the responsibility to fix broken systems and took training for emergency situations. But their plans were not mature or very detailed about response scenarios for situations such as the one they were facing. Operators were not real clear on when to call their ICS vendor, Illinois Electric Systems. Unlike Light for All's plan that required them to immediately call when a blackout occurs, Connected Utilities' response plan was ambiguous about waiting for the vendor to start repairs versus trying to fix the system while they wait. It was also not clear what level of damage was needed in order to call for help. On the cyber front, Connected Utilities did not have any in-house cyber experts trained to analyze and remove malware to get systems cleaned up and working properly again. Instead, they maintained a relationship with a CV1's Chicago office, who came every month or so to examine their systems. Their response plan did not clearly indicate situations when operators should call CV1 for assistance. In fact, Connected Utilities did not have mechanisms to definitely determine when a cyber-attack was occurring. As a smaller entity serving suburban and rural areas of Indiana and Illinois, Connected Utilities was in the process of establishing ties with state and local governments to create paths for assistance and support, but had struggled to finalize these relationships due to the government prioritizing companies with larger and more populated service areas before Connected Utilities. When they finally did call CV1, they faced a similar problem Light for All did, where the knowledge of industrial control systems was limited, and they did not have enough employees to assist the company. (Figure 2)

A Malware Attack Occurred

During the weeks prior to the outage, all three companies had, ironically, been working with third party cybersecurity and operational technology (OT) vendors to upgrade the security of their systems. Following normal procedures, upgraded firewalls, new authentication processes and stronger virus protection systems were installed by the cybersecurity vendors, and OT vendors used remote access to the ICS operations to upgrade their systems and insure they were not impacted by the new, increased security. Remote access was a common way for OT vendors to assess the company's networks and processors, perform maintenance, and run diagnostics remotely.

Unfortunately, a newly created malware, Indestructor, was injected into the energy companies using the same remote access system that the OT vendor used to manage the ICS. The actor (a hacker group) was able to utilize an exploit for the remote access system and install a backdoor to give them maintained access and bypass encryption and authentication measures that were otherwise needed to use these systems. The hacker group actually targeted these three companies due to a similarity in their OT system. They first hacked the vendor to identify where the new OT system was going, and identified Accelerated Grid, Light for All, and Connected Utilities as their targets. They then created malware to attack all three. The hackers were able to access the systems quickly through the backdoors and established a connection between the hacker's external server and the energy company's internal server. They installed the malware, which was capable of taking advantage of the DNP3 protocols used by the infrastructure to control the OT systems and create a new communication process that connected the hackers directly to the utility systems. Indestructor was then able to issue direct commands to a Remote Terminal Unit (RTU) in the grid, which led to a triggered opening and closing of the circuit breakers and caused substations to de- energize, and re-energize, affecting the balance of power in the grid. The malware was eventually able to shut down multiple substations in the transmission system. (Figure 3)

Immediate Effects

Step-down substations lower the voltage so that distribution systems could deliver energy to homes and local buildings. In Massachusetts and Rhode Island, Accelerated Grid's substations worked in conjunction with the distribution system run by Light for All, making up a substantial portion of the grid. With the cascading effects of the malware on the transmission substations, over 1 million people in Massachusetts and Rhode Island were left without power. The malware also disabled any self-correcting or automatic mechanisms that could have normally helped to restart the systems. Data from the utility company's computers were deleted. Furthermore, a Connected Utilities substation also experienced major physical damage which was reported when smoke began appearing from one transformer, likely due to the increased pressure from the erratic behavior of the circuit breakers. (Figure 4)

Immediately following the outage, local businesses and other infrastructure operations began facing serious complications as well. Critical institutions such as hospitals and government buildings had backup generators, but other industries that affected the greater public such as transportation, begin to suffer. In the Northeast, public transportation came to a momentary halt; the subway on the outskirts of Boston were delayed several hours, then came back with limited services using backup generators. Bus service was also impacted as traffic lights and signals switched to back up generators. The outage resulted in prolonged traffic, people having to walk places, and a surge in prices for ride share services. While there are no underground trains in the areas affected in Illinois and Indiana, buses experienced similar delays, leaving numerous people behind their daily schedules.

Another area of concern was the water industry, given that electricity is needed for water plants that deliver clean and safe water to homes. Furthermore, even though backup generators exist in hospitals and other critical buildings, the water comes from outside sources and must be pumped through a system that both sanitizes and delivers water. The disruption in the energy delivery system created a problem for sanitation. Since electricity was cut off in both the Northeast and in the Midwest, millions of people were left without drinkable water. Plumbing also becomes a major concern, and people are forced to find different sources of water in order to use restrooms, showers, sinks and other systems.

Furthermore, the outage also cut phone lines, and those without cell phones were unable to make calls. While longer term concerns included charging batteries for cell phones, those who were able to send messages or make calls were often unable to connect to their target person. Cell towers had backup generators but concerns about how long that would last also arose. This made it difficult for authorities to deliver critical information to people in a timely manner. There was no immediate information released regarding road closures or public transportation delays as well as possible accidents leaving people confused and anxious about safety. Updates on power restoration for the public were made, but how far they reached was uncertain.

Initial Response

With response plans in place, the real time operators on site were instructed to attempt to restore power themselves. However, with the physical damage that occurred, the operators on scene struggled to do so. They were still under the impression that the damage came as a result of too much demand, or a natural cause, much like that of the Northeast Blackout of 2003, where transmission lines sagged into overgrown trees and caused a multiple day outage across the Northeast and Midwest of the country. Within a few hours, Accelerated Grid, Light for All, and Connected Utilities quickly exhausted their initial response mechanisms and managers knew that they need further assistance in order to recover. Each company had a different approach to their response and recovery.

Accelerated Grid quickly received calls from customers about the blackout and reported that nothing out of the ordinary, such as a tree damaging a transmission line, occurred. Industrial control system experts from the company examined the issue. They were unable to trace the cause of the outage and or identify how the substations shut down so quickly. The employees at Accelerated Grid considered the list of possible causes, with cyber threat as an increasing possibility because all data from their computers had been wiped out. The in-house cyber employees were unable to get to the central location quickly. After five hours, their in- house employees arrived and completed their analysis of the systems. They were unable to isolate the malware. The company had not included a response for a data-wiping attack in their response plans and had no current backups for their control systems to help restore power. Their response plans indicated that they would reach out to CMA if something like this occurred, and CMA was contacted. CMA attempted to provide services but was unable to provide enough power to cover the entire outage area, citing distance, transportation, and concern about contaminating other systems with the malware as issues preventing a full-scale alternative energy source. As their response plan stated, the employees also decided to call the DHS fly-away team, who ensured that they would be given assistance as soon as possible.

Light for All faced different circumstances than Accelerated Grid, as their systems were not directly infected by the malware. Since Light for All's distribution substations were directly connected to Accelerated Grid's transmission lines, they experienced an outage in delivery capability but had to wait for the transmission system to be fixed. In the meantime, their response plan for outages required them to reach out to their contracted industrial control experts at Stronger for You. The experts analyzed the effects of the malware on their part of the grid and found that no damage to the substations or lines had occurred. Their customers were without power, but Light for All had no options for using alternative sources to recover.

In the Midwest, the situation was also different. Since Connected Utilities had limited in- house resources, they called their contractors. Since one substation that fed major distribution centers experienced major physical damage, the company's in-house operators were unsure of their next steps. The fire department had been called and the smoldering substation was no longer on fire. The operators attempted to get the power up and running, but due to the recent upgrades in their OT systems, the company did not have a backup transformer readily available. They had a plan to invest in one in the near future, but that was not going to help fix this emergency. They went through the steps outlined in their business continuity plans for restoring power but found that they are unable fix the failed systems. The employees began to consider other root causes for the failure in their control systems. After nearly six hours of analysis and forensics, they heard about the outage in the Northeast where a cyber-attack may possibly have been the cause. They contacted the Chicago office of CV1 for assistance, only to

learn that it would be another five hours before they could reach the site, due to added traffic from the outage. (Figure 5)

Transition to Recovery

First Steps

After a few days, all three companies were able to restore power delivery, and the companies and the grid as a whole were on the road to recovery. Indestructor, the malware, wiped out most of its own footprint, but cyber vendors were able to analyze its effects and study how it was able to take down a major portion of the grid. Officials were called in, and the cause of the outage was released to the general public to assist others should similar issues be noticed.

However, other long-term consequences of the attack were creating new concerns for the energy delivery companies. Top on the list were physical damage and future vulnerabilities. Executives at the three affected companies held emergency executive team meetings to identify resources necessary to avoid similar issues in the future and focused on the steps necessary to ensure that their systems were safe and protected. Working with their OT vendors, the ICS team and their cybersecurity peers removed the backdoor, and installed new authentication measures, patches, and software to decrease the system's vulnerability. Supply chain vendors were given new passwords and procedures for accessing ICS systems. To further prevent a reoccurrence in the future, executives from the energy delivery companies created an organization to make it easier to share information with each other about outages and recovery mechanisms to protect others from an event such as this one.

The other industries impacted by this cyber-attack also had a difficult time recovering. The transportation across the four different states resumed normal services after three days, but the wake of their outage caused citizens and local governments to reexamine their own recovery and response mechanisms. Following this incident, the city transportation departments started brainstorming ways for their services to be more resilient. They planned on installing additional backup generators for power and established relationships with energy specialists should they need additional help. The water industry faced greater complications; without sanitary water, they were forced to create additional partnerships with nearby towns and states to get drinkable water to their citizens, which would be costly. It took a week for normal operations to resume and for the water plants to function properly, as there was heightened fear that the outage may have induced further damage. The communications sector gradually recovered as power was restored area by area. Telecom and cellular service companies also made plans to have additional backup power supplies and larger companies in

the areas of the outages considered plans for alternative telecommunications should their landlines and cell phones not work during an emergency situation.

Luckily, few people were injured as a result of the power outage. Since hospitals had strong backup generators, critical patients were successfully cared for, and other urgent cases that occurred were diverted to hospitals that could accommodate them.

While the local and state government buildings did not lose power, officials began thinking about damage to critical infrastructure and how to aid the utility companies next time. Topics of discussion ranged from establishing closer relationships with critical infrastructure companies, changing standards for response mechanisms, local coordinating boards to assist in emergency situations, review of regulations that might assist or inhibit response and recovery, and additional planning and response processes for officials.

Future Planning

In the meantime, the ESCC decided to convene a meeting to discuss the Indestructor event, given that it was the first large-scale cyber-attack on an industrial control system in energy delivery subsector of the U.S. Even though the utility companies responded to and recovered from the attack, the ESCC believed that the process could have been more efficient and effective in practice. What could the ESCC do to assist utility companies, so this type of malware attack did not happen again? How could the ESCC assist utility companies of all sizes and capabilities with their cybersecurity response and recovery plans? Indestructor was an attack that impacted two different utility companies in geographically different regions at the same time. Resources were spread thin. Some expected resources were unable to assist in this situation, given the broad geographic impact. The ESCC begins to evaluate the likelihood that this would occur again.

Their meeting led them to questions regarding response mechanisms in mitigating the attack that extend beyond a single, or even two companies. Since another large-scale attack could happen again, the ESCC focused on the ecosystem's response as a whole. They sought to answer one question: How can all companies be prepared for a cyber-attack? They decided that the response plans needed to include more detail, but what was the most appropriate mitigation plan?

FIGURE 1: OVERVIEW OF FICTIONAL UTILITY COMPANIES IN THIS CASE STUDY

Name	Locations Served	Description
Accelerated Grid	Greater Boston Area, mainly Southeast Massachusetts, Providence, RI	Transmission Company
Light for All	Greater Boston Area, mainly Southeast Massachusetts Providence RI	Distribution Company
Connected Utilities	Illinois and Indiana	Transmission and Distribution Company

FIGURE 2: RELATIONSHIPS BETWEEN UTILITY COMPANIES AND EXTERNAL SOURCES OF AID

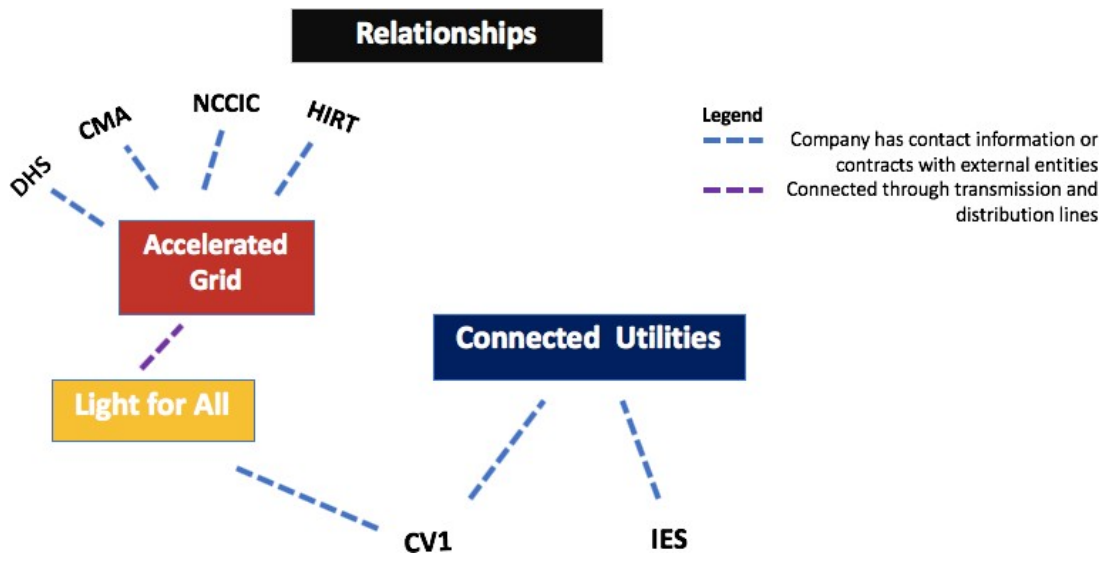

FIGURE 3: MALWARE ATTACK OUTCOME

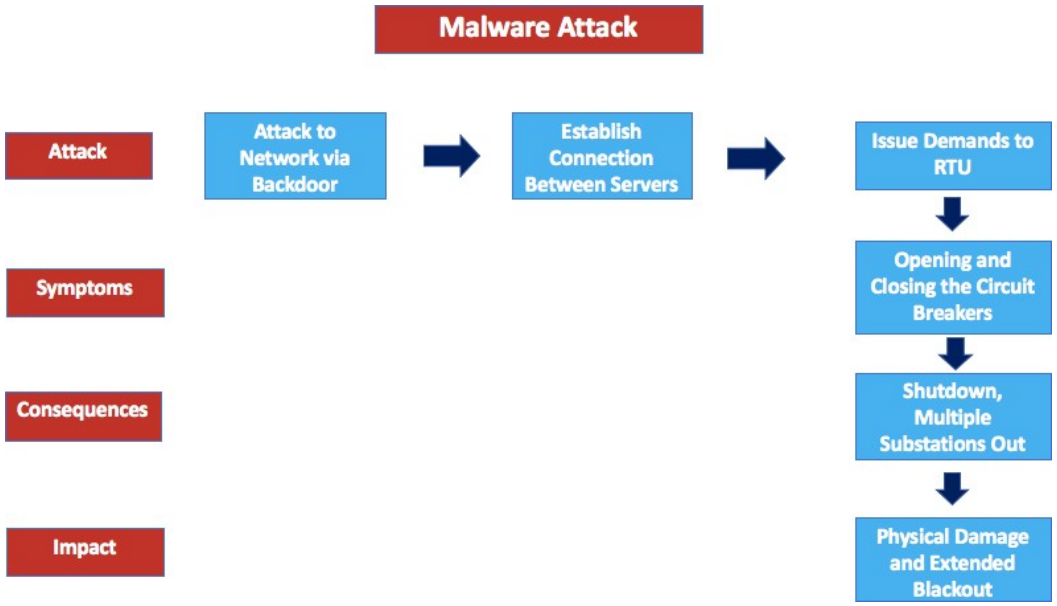

FIGURE 4: IMMEDIATE IMPACT ON ELECTRICITY GRID

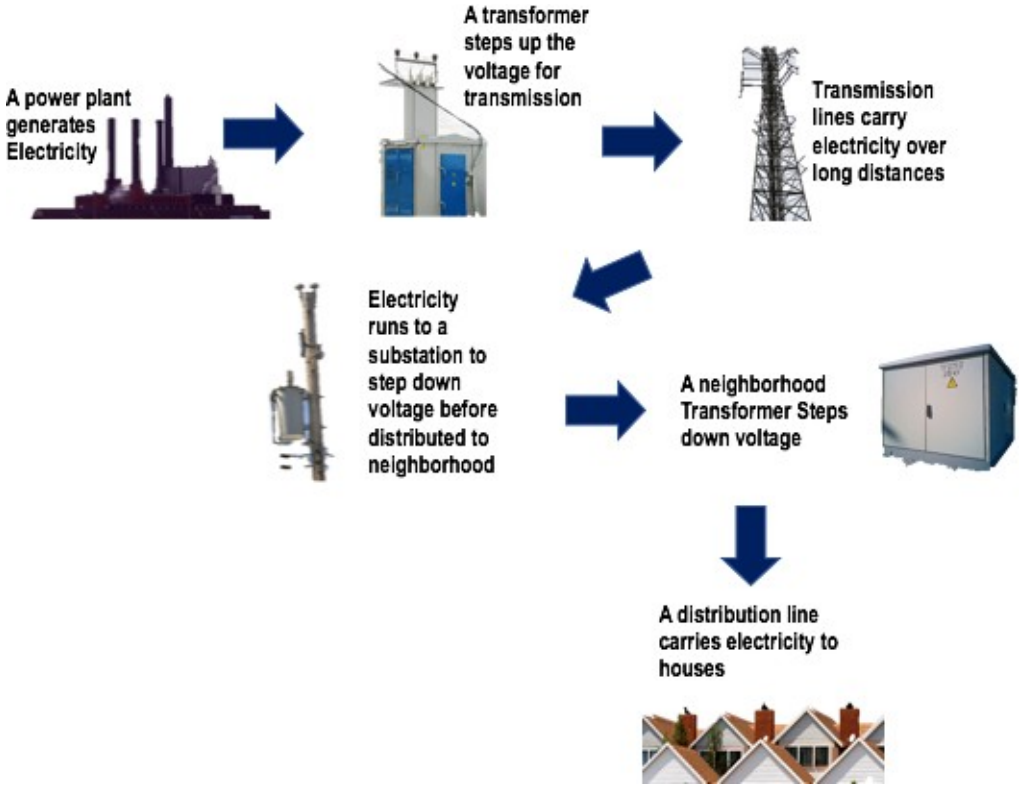

FIGURE 5: INITIAL RESPONSES BY COMPANIES TO MITIGATE ATTACK

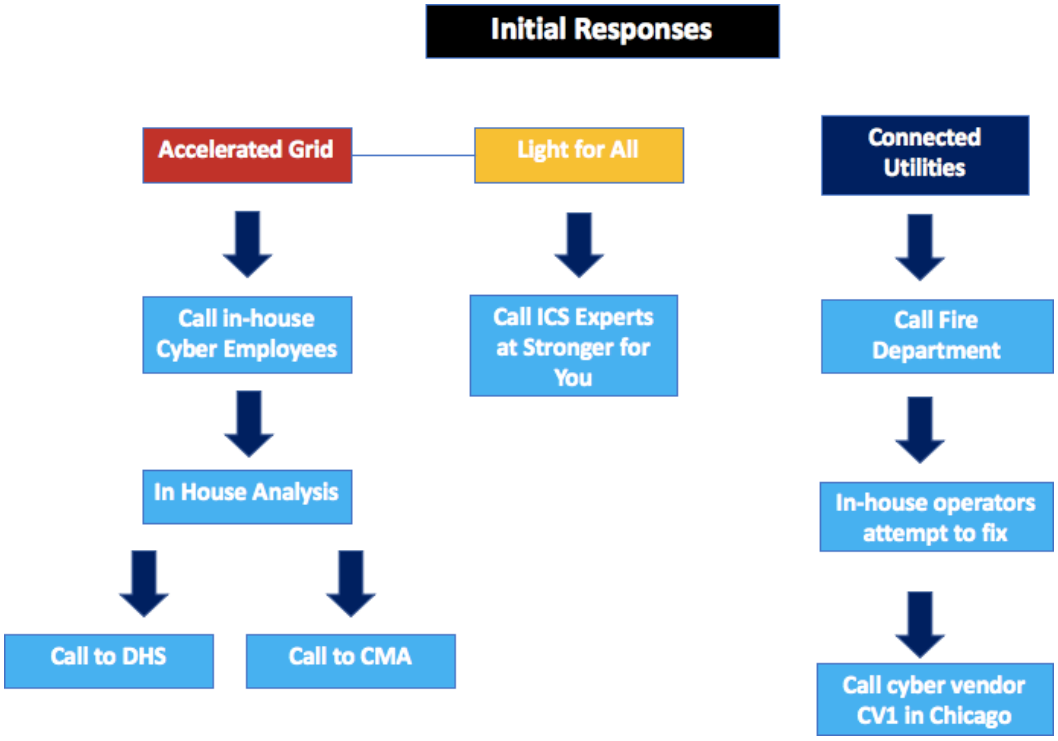

FIGURE 6: ACRONYMS USED IN CASE STUDY

Acronym	Full Name
IoT	Internet of Things
IT	Information Technology
OT	Operational Technology
MISO	Midcontinent Independent System
NERC CIP	North American Energy Reliability Corporation – Critical Infrastructure Protection
CMA	Cyber Mutual Assistance
ESCC	Electricity Subsector Coordinating Council
DHS	Department of Homeland Security
NCCIC	National Cybersecurity & Communications Integration Center
HIRT	Hunt & Incidence Response Team
ICS	Industrial Control System
RTU	Remote Terminal Unit
DNP3	Distributed Network Protocol 3
CV1	Cyber Vendor One
IES	Illinois Electric Systems

Preparing for a Large-Scale Energy Delivery Sector Cyber Attack

Teaching Note*
December 31, 2019

Overview: This case was written to illustrate the gaps in the electricity sector's response to a major malware attack, given its the interdependencies with other critical infrastructure sectors and specific requirements, the increasing likelihood of such an attack, and the unique requirements to respond to an attack at scale. It is intended to generate discussion regarding the entire electricity ecosystem's participation. The case is driven by hypothetical scenario based off a real malware, Indestructor (based on the real life malware incident known as CrashOverride), that targeted Ukraine's power grid in late 2016.

The discussion with the participants should highlight these key points:

1. An attack on the United States electricity grid is more than likely to occur in the near future, especially as the electricity sector's infrastructure becomes increasingly digitized and hackers become smarter and create malware that is targets the numerous vulnerabilities in industrial control systems.
2. Electricity companies in the United States are subject to a multitude of regulations, including NERC CIP and various state regulations, that govern their response preparation, but these standards are inconsistent and may lack the necessary elements that a company must include to be prepared to limit the effects of a large-scale malware attack.
3. As a whole, individual response plans are not tested rigorously enough to model real-world conditions, and companies cannot assert that they are prepared in the event of an emergency. But even if company responses are in place, there are gaps between companies that are a vulnerability to the entire ecosystem that must be discussed and planned for.
4. Second and third order effects that will result from a power outage can be severe, especially when the water, telecommunications, and transportation industries are affected.

Teaching Plan:

Study Questions:

1. Consider the electricity sector as a whole ecosystem. What are the holes in the ecosystem's mitigation preparedness for responding to Indestructor?
2. What areas require greater collaboration and better response mechanisms for malware mitigation?
3. What would you list as the top 3 priorities for the electricity ecosystem to cope with a large scale cybersecurity breach such as Indestructor? What role should companies like Accelerated Grid take? Companies like Connected Utilities? What other organizations/agencies need to be involved in realizing your 3 priorities and how?

* This teaching note was written to provide instructors with a teaching plan for the case study "Preparing for a Large-Scale Energy Delivery Sector Cyber Attack" (by Dr. Keri Pearlson, Michael Sapienza and Sarah Chou, December 4, 2019). This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Introduction (to read to the class): Cyber-attacks are happening more frequently each year, and numerous industries have already faced the effects of malicious actors. The electricity sector is one of them. Despite significant investment in resources (time, planning, funding, technology, and strategy), the sector still faces significant vulnerabilities and response plans are not ready for catastrophic cyber attacks.

While many of the cyber issues are technical in nature, many are not technical. No organization is 100% secure and all computer systems can be hacked. Cybersecurity vendors provide many different types of barriers, detection systems, recovery plans, and more to help energy companies protect their systems. But today's cyber-attacks occur largely due to a lack of knowledge about existing vulnerabilities and the rapid creation of avenues of attack that exploit new ones.

The convergence of IT and OT (Operational Technology) in the energy sector have created new zero-day exploits, and cyber threats that target a large-scale attack that affects multiple companies is becoming increasingly real. Today malicious attackers target systems that can be compromised by faults in the organization responding to these events.

In this case study, we are going to examine a fictitious malware attack on the electricity sector. We will look at how two companies are prepared, how they respond, and how the entire ecosystem is impacted. The malware, Indestructor, is fake, but the story is based on real life events that happened a few years ago. Our goal today is to highlight the ecosystem response mechanisms: even if companies are prepared, there are still holes in the ecosystem plans that can keep the sector from recovering in a timely manner. Our goal today is to get the discussion going so the key players in the ecosystem can work together to address these holes and create plans to plug them.

BACKGROUND/INTRODUCTION

1. Let's start by understanding the electricity sector. Who are the key players and what is their role in the day to day offering of energy to the US? (probe for types of players, not necessarily company names…if company names, list them but pull together these types of players from the discussion):
    a. Large Utility companies (like Accelerated Grid)
    b. Small Utility companies (like Connected Utilities)
    c. Federal Government entities (DHS, FBI, Dept of Energy, DOD)
    d. Ecosystem organizations (CMA)
    e. Cybersecurity vendors
    f. Local, State, government
    g. Universities/Research orgs (some national labs work on energy sector cyber)
2. What would be their role in the event of a cyber attack/malware attack?
    a. Large utility companies: On-site operators and industrial control expert teams should handle any damage, and their cyber experts are responsible for diagnosing the problem. Essentially their team would be the ones who try to fix the issues first. If they cannot fix it, then they would call external help such as vendors or government agencies. In this case: Accelerated Grid.
    b. Small utility companies: Because they are smaller, they are focused on the coordinating external help by following their response plan. This includes calling their contracted vendors. In this case: Connected Utilities.
    c. Federal government entities: Assist as requested by utility companies or state government – the government must be called in order to give aid. Government entities would include

FBI, DOE, who would send in teams with resources. This includes experts on cybersecurity, physical damage repair, and connecting to other agencies for help.

d. Ecosystem organizations: When called by utility companies, they provide resources in the form of personnel, software, etc. Example from the case is Cyber Mutual Assistance, who's participants attempted to provide aid but could not due to a number of reasons. Transportation delays and concern about contaminating other systems were two of them.
e. Vendors: Provide cyber assistance to utility companies who call them for help. Vendors such as CVI would most likely be on contract and provide cyber analysis and any other aid such as new firewalls, software, etc.
f. Local or State government: Most likely, they don't have coordinated response for this type of malware attack.

3. What in your opinion is the biggest concern for the ecosystem?
    a. Sample answers: No cooperation among the different levels of actors/stakeholders within the ecosystem to effectively respond to a cyber attack. Lack of clear distinctions on who helps who and when, especially when multiple areas of the ecosystem are down. Companies are hesitant to share information for fear of reputation harming, vulnerability.

CYBER ATTACK ANALYSIS

1. What was Indestructor and what did it do to the energy companies it affected? (paragraph 15 &16)
    a. Indestructor was a malware created to target ICS systems, able to get into the system through a widely used protocol.
    b. Malware triggered circuit breaker issues and shut down multiple substations within the Accelerated Grid transmission system. Cascading effects ultimately shut down the connected Light for All distribution lines, cutting power off to millions of people.
    c. Connected Utilities experienced the same thing, but they were the only company affected in the area.
    d. Malware also disabled any self correcting or automatic mechanisms, in addition to wiping its own footprint.
2. Probe: Let's look at Accelerated Grid in a bit more detail. What happened here? How did they respond? (paragraph 21)
    a. After attempting to examine the issue themselves and then considering a cyber attack, the in-house cyber employees were called in to analyze their system.
    b. They reached out to CMA because their response plan did not include backups to their system to restore power, but CMA didn't have enough resources (transportation, people) to help them
    c. Called DHS fly-away team for help, and received help after they arrived
3. Probe: Let's look at Connected Utilities. What happened to them? How did they respond? (paragraph 23)
    a. The same damage occurred for Connected Utilities in terms of the outage and damage to the cyber systems.
    b. Physical damage was first taken care of, then attempted to fix the system themselves by following their business plan
    c. They contacted their cyber vendor, CV1, after hearing that a cyber-attack may be the source of the outage. While this is usually the very last step in diagnosing an issue, the delay in contacting the vendor means that the malware has time to spread or have a greater impact on the systems. Best case, it delays getting a patch or fix for the systems from the vendor.

4. Who from the government responded and what did they do?
    a. Government is only allowed to aid when they are called, so they were only able to aid Accelerated Grid.
    b. Connected Utilities hadn't established a relationship with a government entity yet, so they didn't know who to call or when to call
    c. Only the DHS team was a part of this response effort in the ecosystem, and sent in a fly-away team with resources. We would assume that the DHS team would provide aid in terms of providing experts to restart the systems, analyze the malware, and eventually perform forensic analysis.
5. Who else responded?
    a. Cyber vendors and other assistance agencies (CMA) were part of the responses in this ecosystem. However, they were called too late and faced complications in helping their respective companies.

Summarizing the impact of this attack, we can see that individual companies responded to the best of their abilities, but there were still impacts. Some of those impacts might have been avoided with different planning.

IDENTIFYING THE ECOSYSTEM HOLES TO RESPONDING TO A MALWARE ATTACK AND PLUGGING THEM

6. What holes do you see in the response to Indestructor?
    a. All actors are doing their job, but there is no coordinated effort where each part of the system is aware of their role in relation to others; there is no standard for what a response for the ecosystem looks like, where people know when to give aid and who to give it to.
    b. Those who want to help are often left without resources, due to financial or bureaucratic issues. People are expecting help.
7. How would you recommend plugging these holes?
    a. Students might come up with several approaches to this:
        i. Sample answer: The electricity grid is a national issue, and thus the government can take the initiative to plug the holes. One option is through creation of a new agency to regulate the electricity ecosystem. Holes can be plugged once a unified response plan for the entire ecosystem outlines what each part of the system does and how it makes up a greater whole.
        ii. Another answer: key players in utility companies take their own initiative to come up with an ecosystem wide response plan. Similar to the financial industry's regulation.
    b. Increasing communication and information sharing on issues regarding how the utility companies interact with vendors and government entities and how they interact with each other.
8. Where did the government entities assist? How would you evaluate their response? What would have improved their response?
    a. Utility commissions expect help from the federal government, but this only comes as a result of the utility companies having relationships with the entities. Smaller companies such as Connected Utilities couldn't access these resources because they were working to get government support, which larger companies receive priority.
    b. The DHS fly-away team assisted Accelerated Grid as soon as possible in this case, but only after they were called.
    c. Their response was done well according to their policies, but the larger issue about the

ecosystem and the question of who they help emerges. If they only have so many resources, there needs to be an effective way to decide who gets help when multiple parts of the grid are down.

d. There are other government agencies such as the FBI, DOE, HIRT that could be helpful if the utility companies included them in their response plan.

9. Where did the CMA assist? How did CMA assist? How would you evaluate their response? What would have improved their response?
    a. CMA attempted to provide their services but ultimately did not assist any of the utility companies. Their response would have been improved if they had more resources, perhaps as a result of more government aid and help for providing these things.
    b. There is a concern about contaminating other systems in addition to giving away any resources that individuals might need in the future. Having some sort of coordination with other agencies or vendors so that the responsibility is shared would be ideal. This way, CMA is aware of what is available and how they can help.
    c. Outside of this scenario, we can assume that CMA would provide aid in the form of sending experts to assess the cyber attack (determine when the systems are safe to use again), volunteer software to get the system back and running.

To summarize this part, we can see that there are disconnects within the ecosystem. Some entities do not have the resources to do what SHOULD be done. Others expect support from entities that do not have resources to cover everyone at the same time.

SUGGESTIONS FOR THE FUTURE

10. What would you advise execs at Accelerated Grid to do?
    a. Executives at Accelerated Grid should continue to establish relationships with other government entities (FBI, DoE), vendors, and ecosystem organizations.
    b. Their response plan should be more specific on the role that each of these players would have in case of a cyber attack.
    c. Would advise the executive to do an exercise or stress test of the response plans that goes beyond their own internal efforts. Audit this response plan to ensure that it can handle any unexpected issues (phone lines down, internet down).
11. What would you advise execs at Connected Utilities to do? More specific maybe something about local state FBI agencies
    a. Since they have less in-house resources, they need to prioritize what they do in order to improve their response plan.
    b. Executives at Connected Utilities should push for connections and partnerships with government entities. They need these entities in case of an emergency and their vendors who are limited in their resources are unable to help.
    c. Specifically, local and State FBI connections need to be established. Because Connected Utilities is a regional company, they can rely on these local divisions during the response phase.
    d. They should also do a stress test with how they respond given their limited resources and connections.
12. What policies or additional government mechanisms are needed?
    a. Very broadly, there needs to be some government regulation that clearly states what should happen in the event of a cyber attack on the ecosystem. There needs to either be policy or a standard that states a uniform response across the grid, where the utility companies, vendors, organizations, and gov entities know what they need to provide and

what others are doing

b. One example would be: adjustments in the NERC CIP standards that potentially outline specific guidelines for utility companies' response plans at each step of an attack and the role that external help must play. In other words, requiring that each level of the system is helping out.

13. Who should be in charge of coordinating the ecosystem response? Why? What would coordinated response look like?
    a. Several angles that students can take: The federal government needs to take charge of coordinating the ecosystem response because this is a potential issue that would affect the whole country. Furthermore, only the government has the resources to organize a wide scale response mechanism. It is the DOE's responsibility to ensure the safety of the electricity grid in the US.
    b. Utility companies: leaders of the largest utility companies coordinate amongst all companies, vendors, and government entities to facilitate the response plans/interaction between all. This way, they could ensure that regardless of utility company size, the ecosystem can respond accordingly.
    c. Vendors: Vendors (such as CV1 from the case) in charge would focus on ensuring that resources for mitigating an attack exist for companies. They could potentially require that all companies have a relationship/contract with a vendor that could help them when they need.
    d. Governors: all state governors come together and determine a response plan that connects federal and local responses, as well as the different regulations that each state may face.
    e. A coordinated response would look like: a cyber attack occurs, and all levels of the system are aware once it has been diagnosed. Each part (vendor, organization government) sends in their teams where needed. All utility companies regardless of size have contacts for these external aids, and those trying to help have enough resources or ways to obtain the resources from partner organizations or the government.

CONCLUDING THE DISCUSSION

There are several key points to take away from this discussion:

1. While individual companies may have well thought out response plans (and that is not a given), but there are gaps in the electricity sector's ability to respond to a large-scale malware attack. The response mechanisms for the ecosystem as a whole are not well defined nor clearly articulated. Response organizations are tied together but the specific roles for each participant are not clear or are redundant. There are jurisdictional overlaps.
    - In this case, the entire response scenario is fragmented. Even though the same attack was occurring in two different areas, the response for each was largely different and dependent on the individual company.
    - There are only solutions for individual companies, but none that point to helping the ecosystem as a whole. There is no government or industry directed aid that helps everyone involved.
    - The roles of the DHS, CMA, and HIRT overlap, in that all three are able to respond but what are their roles? Their form of help is not specified, even in the Accelerated Grid plan.

2. (Vendors and Facilities) There are a number of measures that can be improved and a number of new response mechanisms that might be created to address this ecosystem-wide issue. In general,

there is a disconnect in the ecosystem agencies (vendors specifically) that help in responding. The mechanisms that do exist are not well tested and effectiveness is not adequately measured.

- CMA is one response mechanism that can be improved. It is not effective because people face restrictions on transportation and resources, especially when they might not want to give up their cyber resources.
- Companies expect response from vendors such as CMA, other for-profit vendors, CV1 has offices in Chicago and Boston but only have so many resources for their customers and they have to decide who to help when there is an ecosystem-wide problem.

3. (Company) There is a large disconnect for support for critical infrastructure companies. Larger companies have more resources for response than smaller companies.
    - Larger company such as Accelerated Grid has contacts at the DHS, CMA, HIRT, that would aid them in response given that resources are available. They also have in-house resources such as cyber experts to first examine and diagnose the issue.
    - Smaller company such as Connected Utilities has considerably less resources. They don't have any in-house cyber experts that would allow them to recognize the problem first, but instead call their cyber vendor for assistance in this scenario. They do not have any contacts through CMA or at DHS that could support them if an attack were to happen. Want to make changes but cannot due to lack of funding.
    - People in general are unable to respond because of the lack of support.

4. (Government) All companies expect some support/assistance from government groups at both the state and national level, but those resources may not be available at the time of an ecosystem-wide issue. Regulatory and government models struggle to keep pace with threats. Response strategies, processes and frameworks are not integrated geographically between state and federal and between public and private organizations. Mechanisms and people are not trusted at the level necessary to adequately respond.
    - Government groups must be called in order to send a fly-away team, they can't immediately respond without the request. As in this case scenario, Accelerated Grid called the fly-away team and were informed that help would be coming as soon as possible.
    - In a large-scale attack on the whole ecosystem, the number of people or fly-away teams may be limited, and the government is then left with the question of who to serve.
    - Companies expect help, but they must establish an existing relationship, so they are able to access it.
    - Connected Utilities was working towards getting support from the government, but the government was prioritizing larger companies with more populated service areas.
    - Each state also has their own individual aid that is coordinated exclusively from others. What happens when the outage across state lines? Do companies know how the state interacts across state borders? In this case, the outage is happening in multiple states and the states do not know how to help.

5. Few companies/organizations are empowered to make changes to improve cyber response mechanisms, and those with the ability to do so are not actively creating these mechanisms. Each part of the ecosystem can do their job to the best of their ability but can't do much more when it comes to coordination and response on a system wide level.
    - In our case, all of the companies, vendors, and government are doing their part in the response, but none are charged with filling the gaps between the system
        1. Companies only have so much they can do in terms of response
        2. Vendors and facilities are limited by who they are and what they do: resources are

limited and how do they prioritize who they serve?
3. Government has control over resources but require a lot of bureaucracy to make mechanisms work and put them into action. Requires public voter support to approve any changes in infrastructure costs.

- There is no coordinated effort where each part of the system knows who is giving aid when and what to give where and no standard for what a response looks like.
- The government would need to know how to fill the gap first, perhaps through new regulation that would tie all parts of the system together or a new entity.
- No federal requirement for individual utility plans to include response mechanisms from each level of the system.

BACKGROUND FOR ADDITIONAL LECTURE: REAL CYBER EVENTS (all are industrial control systems (ICS) tailored malware attacks)

1. Indestructor/CrashOverride:
    a. Basis for our scenario, occurred in Ukraine in 2016, largest cyber-attack on industrial control system and is not exclusive to vendor specific software or systems – can happen to anyone.
    b. Affected transmission level substation, where the malware was able to access the network by taking advantage of commonly used protocols cause breakers to open and close, and ultimately result in a system shutdown and a prolonged power outage
    c. The malware analyzed by Dragos reveals that multiple types of attacks can occur, namely de-energizing a substation and forcing an island event
    d. Malware is also known to include a data wiper module, in which it can erase all of the files in the system that it affected
2. TRISIS/TRITON
    a. Attack on Middle Eastern plant whose vendor is Schneider Electric in 2017, occurring during the weekend at a time when the plants are relatively understaffed
    b. Malware caused emergency oil refinery plant process system shutdown, also known as a malware that was "built to kill"
    c. Worries are as such: malware attacked through the industrial control system, so if others have a similar system, they can easily fall under attack by the actors. The malware is known to target Schneider Electric's Triconex Safety Instrument System. Once safety controls are defeated, the malware can cause physical damage and environmental damage, while hiding its own presence under the guise of safe files.
    d. Malware had a second resurgence in early 2019, and its full capabilities and potential severity are still to be seen, as believed by many people.
3. HAVEX
    a. In 2013, Campaign targeting the ICS used across multiple industries, through phishing campaigns and also redirected websites – anyone could have been able to cause this to occur.
    b. Able to gain access to systems to gather information, targeted and impacted more than 2,00 sites in total within the U.S. and Europe, notably energy grid operators, electricity generation firms, and aviation, defense, and pharma industries
    c. Malware leveraged Open Platform Communications, a protocol that many ICS facilities use particularly in Europe.
    d. Intended espionage rather than any other type of damage – how does this change response plans if at all.

Cybersecurity at MIT Sloan
Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity
Case Study

Preparing for a Large-Scale Energy Delivery Sector Cyber Attack*

December 4, 2019
Dr. Keri Pearlson
Michael Sapienza
Sarah Chou

[1] Keeping the infrastructure of the country safe and secure is a non-negotiable need, but these same systems are constantly being targeted by cyber criminals' intent on disrupting operations. Though the United States electricity grid is considered to be safeguarded and reliable, no system is impermeable. While the grid regularly faces system failures and effects of natural disasters one threat that the United States electricity sector has yet to face is a large-scale cyber-attack that has catastrophic consequences. This is good news. But at the same time, cyber-attacks on all industries are becoming more frequent and the threat to the energy sector is no different. In the first three months of 2018, there was a 32 percent increase in cyber- attacks on US industries from the previous year.[1] Within the first six months of 2019, over 4 million data breaches occurred.[2]

[2] While all cyber-attacks are of concern, the unique concerns for the electricity sector lie in the potential for a large-scale attack where multiple utility companies are hit simultaneously, or an attack on a critical utility company where there are compounding effects on others that cause a domino-like impact across the sector. The result of either of these types of attacks would be a crisis for the impacted utility, but in addition, there would potentially prolonged outages or other damages since there might be insufficient resources available to assist in recovery and returning to normal operations.

---

* This hypothetical case study was prepared by Wellesley student Sarah Chou, MIT student Michael Sapienza and MIT CAMS Executive Director Dr. Keri Pearlson for discussion and teaching. Any resemblance to any real organization is purely accidental. The authors would like to thank Hans Olsen, Mike Steinmetz and several other reviewers who asked to remain anonymous. Thank you to contributors Jess Smith from Pacific Northwest National Laboratory, Scott Baker, Jonathon Monken and Steve McElwee from PJM Interconnection, and Jake Schmitter from Electricity Information Sharing and Analysis Center (EISAC) and a number of other contributors who also asked to remain anonymous. This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

[1] https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/

[2] https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#48247dcebd54

[3] Cyber threats increase due to the evolution of technology. Newer developments such as the internet of things (IoT), the cloud, smart grid tech, and IT/OT convergence are intended to increase efficiency and replace outdated systems, but they also introduce gateways for possible attacks. IoT specifically is quickly becoming more vulnerable, with nearly 3 billion cyber-attacks recorded as of September 2019.[3] When everything is connected to a network, even one that is 'air gapped' from the Internet, it becomes easier to bring down the whole system with a well-placed cyber-attack. Further, as innovations arrive at an increasing pace, it also becomes even more difficult for managers to adapt operations and response plans to keep pace with dynamic changes.

[4] For many, it's not a matter of 'if a major attack will happen' but instead "when," and how to prepare for the "inevitable" as MIT Professor Stuart Madnick says.[4] Hackers are becoming smarter, constantly finding new ways to launch attacks, and defending against the unknown is difficult, if not impossible. Just follow the press, where many examples of countries such as Ukraine and Saudi Arabia faced cyber-attacks on industrial control systems in the energy delivery ecosystem. Should that happen in the U.S., the real effects of a cyber-attack on the energy delivery sector can range from momentary power outages to catastrophic physical infrastructure damage. The ramifications of a cyber-attack also reach further than the effects to the grid itself, threatening other critical infrastructure ecosystems such as the transportation industry, the water supply, and the economy as a whole.

[5] Consider this hypothetical case study and the potential wide-reaching ramifications. On an average day in July where the electricity grid was functioning normally, areas of Massachusetts and Rhode Island began experiencing power outages. It was quickly identified that the areas affected belonged to two companies that serviced consumers across the two states: a transmission company Accelerated Grid and distribution company Light for All. Together, the two companies were responsible for power in parts of the Greater Boston Area and Providence, and most of southeast Massachusetts. The cyber-attack resulted in damage to a step-down substation run by Accelerated Grid, which ultimately affected the connected Light for All distribution lines. Within a few minutes, 1 million people were experiencing blackouts, and the number was growing. A short while later, states in the Midwest, namely in Illinois and Indiana also began experiencing power outages. Only one company, Connected Utilities, was affected in this region, though their transmission lines were connected to their own distribution substations responsible for bringing power to residents in cities such as Bloomington and Effington. Around 150,000 people lost power in that region. (Figure 1)

[3] https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#247336685892
[4] https://hbr.org/2017/05/preparing-for-the-cyberattack-that-will-knock-out-u-s-power-grids

[6] The companies initially believed the outages were a result of a system failure and began the normal detect and recover processes. It took five hours to diagnose the cyber-attack. Given that cyber-attacks are not constrained by geographical boundaries, the threat actors were able to target these two completely different highly-populated geographical areas without much effort.

[7] Prior to this, neither the southern Midwest nor eastern Massachusetts and Rhode Island had ever experienced major disturbances to the grid, since like most utility companies, their local suppliers had taken a proactive role to ensuring that the grid was as strong and stable as possible. The companies contracted with vendors to make sure their software was up to date and they had already begun to phase out old and vulnerable equipment. In addition, they also had strong, consistent network monitoring and cybersecurity processes. In the event of an anomaly in their network, retainers with third-party cybersecurity platform vendors kicked in. The companies involved believed they were protected against an event like this up until now.

Preparation

[8] All three companies had response plans that outlined responsibilities for real time operators to restore power. The employees also went through training that taught them what to do during an emergency situation. As transmission companies, Accelerated Grid and Connected Utilities were subject to the NERC CIP standards, which describe standards for transmission companies that include aspects of required training, incident reporting, and vulnerability assessments, among other things. Part of the standards requires companies to train employees on items such as identification and recovery of cyber incidents, all intended to prepare for an attack on critical infrastructure.[5] Because CIP standards do not specifically state the required preparation metrics, leaders at the companies felt they were prepared for a cyberattack, but in reality, they had never performed a physical response drill. Their preparation had been table top exercises or communications exercises which did not simulate real time effects of a cyberattack, such as loss of communications, limited access to in-house expertise, or response to physical damage. In addition, they had not practiced recovery with their vendors, and while they knew who to call they did not have additional plans in place should their standard vendors be unavailable or unable to assist. On the other hand, Light for All as a distribution company falls under the jurisdiction of state governments, which focuses on ensuring that the state offers aid to companies in need both in its resilience plans and response efforts. However, all states have different standards and there is inconsistency in the way they are organized and presented.

[5] https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-004-6&title=Cyber%20Security%20-%20Personnel%20&%20Training&jurisdiction=null

BACKGROUND ON THE UTILITY COMPANIES

Accelerated Grid

[9] Like most utility companies, Accelerated Grid had in-house teams responsible for spearheading response efforts when emergencies occur. On-site operators were familiar with all aspects of their substations and received training on how to manually fix all parts of the system when something failed. They also had a team of industrial control experts to handle damage or disruptions to substations. Accelerated Grid had recently hired two cyber experts that specialized in diagnosing and analyzing cyber problems to find the root cause. As a larger company responsible for supplying power to parts of major cities including Boston and Providence, Accelerated Grid also had sophisticated network monitoring capabilities, which allowed them to recognize issues relating to server connections, end point failures and other potential network issues. The company also had trained their teams with simulated cyber-attacks on their system, to ensure that the experts were familiar with the available resources.

[10] One initiative in the cyber plans for Accelerated Grid was the Cyber Mutual Assistance (CMA) program, the Electricity Subsector Coordinating Council (ESCC)'s program dedicated to aid in the event of a cyber emergency.[6] Accelerated Grid expected CMA to send personnel and equipment in the event of a cyber emergency, as their network of experts offered specialized knowledge on these critical issues that Accelerated Grid employees did not have. However, CMA faced similar limitations in resource availability as other vendors. Transportation and quantity of energy to affected utilities was available but in a limited manner and for a short time. Long term or widely impacted geographical attacks would severely tax the CMA support. CMA is also limited due to the nature of cyber-attacks; lack of geographical boundaries leaves nearly every company vulnerable to the threat, and many may not voluntarily lend their resources in case they may get hacked in the near future. They are supposed to seek CMA help when their in-house cyber employees have exhausted their knowledge in the problem at hand, though there is no objective time in which they should call.

[11] As a larger company, Accelerated Grid maintained a direct relationship with the Department of Homeland Security (DHS). The relationship included an agreement that in the event of a situation where it was needed, DHS would send a fly away team to aid in restoring power. In their plan, employees at Accelerated Grid worked with the National Cybersecurity & Communications Integration Center (NCCIC) and the Director of the Hunt and Incident Response Team (HIRT) in the event that all other internal operations to restore power failed, or if the situation became too severe for the in-house teams to handle.

---

[6] http://www.electricitysubsector.org/-/media/Files/ESCC/Documents/CMA/Cyber-Mutual-Assistance-Program-One-Pager.ashx?la=en&hash=785A8D66D3F21234FF0584FBA026A240FE123130

Light for All

[12] Though Light for All's distribution system is connected to Accelerated Grid, the two were separate entities and did not share resources when it came to response mechanisms. Light for All's response plan however, similarly included on-site operator training on repairs to the substation and specific parts of the transformer systems. However, their response plans stated that they needed to call Stronger for You, their industrial control systems vendor, for help with repairs in the event of a blackout. Light for All did not have any in-house cyber employees. Instead they had a relationship with a CV1, a cyber vendor who was on contract to identify, respond and assist in recovery from a cyber-attack. However, their plans did not clearly state when the employees should call the cyber vendor for help. Managers used CV1 primarily for issues with data breaches or hacks in their corporate office. While their contract had provisions for assistance in the event of an attack on their industrial control systems, CV1 expertise in industrial control systems was limited. CV1's Boston office had 10 employees on call to assist customers with cyber-attacks, including Light for All.

Connected Utilities

[13] Connected Utilities' response plan for emergencies relied on external help, given the limited amount of resources and personnel trained to handle blackouts and potential cyber-attacks. Like the other two companies, operators at Connected Utilities had the responsibility to fix broken systems and took training for emergency situations. But their plans were not mature or very detailed about response scenarios for situations such as the one they were facing. Operators were not real clear on when to call their ICS vendor, Illinois Electric Systems. Unlike Light for All's plan that required them to immediately call when a blackout occurs, Connected Utilities' response plan was ambiguous about waiting for the vendor to start repairs versus trying to fix the system while they wait. It was also not clear what level of damage was needed in order to call for help. On the cyber front, Connected Utilities did not have any in-house cyber experts trained to analyze and remove malware to get systems cleaned up and working properly again. Instead, they maintained a relationship with a CV1's Chicago office, who came every month or so to examine their systems. Their response plan did not clearly indicate situations when operators should call CV1 for assistance. In fact, Connected Utilities did not have mechanisms to definitely determine when a cyber-attack was occurring. As a smaller entity serving suburban and rural areas of Indiana and Illinois, Connected Utilities was in the process of establishing ties with state and local governments to create paths for assistance and support, but had struggled to finalize these relationships due to the government prioritizing companies with larger and more populated service areas before Connected Utilities. When they finally did call CV1, they faced a similar problem Light for All did, where the knowledge of industrial control systems was limited, and they did not have enough employees to assist the company. (Figure 2)

A Malware Attack Occurred

[14] During the weeks prior to the outage, all three companies had, ironically, been working with third party cybersecurity and operational technology (OT) vendors to upgrade the security of their systems. Following normal procedures, upgraded firewalls, new authentication processes and stronger virus protection systems were installed by the cybersecurity vendors, and OT vendors used remote access to the ICS operations to upgrade their systems and insure they were not impacted by the new, increased security. Remote access was a common way for OT vendors to assess the company's networks and processors, perform maintenance, and run diagnostics remotely.

[15] Unfortunately, a newly created malware, Indestructor, was injected into the energy companies using the same remote access system that the OT vendor used to manage the ICS. The actor (a hacker group) was able to utilize an exploit for the remote access system and install a backdoor to give them maintained access and bypass encryption and authentication measures that were otherwise needed to use these systems. The hacker group actually targeted these three companies due to a similarity in their OT system. They first hacked the vendor to identify where the new OT system was going, and identified Accelerated Grid, Light for All, and Connected Utilities as their targets. They then created malware to attack all three. The hackers were able to access the systems quickly through the backdoors and established a connection between the hacker's external server and the energy company's internal server. They installed the malware, which was capable of taking advantage of the DNP3 protocols used by the infrastructure to control the OT systems and create a new communication process that connected the hackers directly to the utility systems. Indestructor was then able to issue direct commands to a Remote Terminal Unit (RTU) in the grid, which led to a triggered opening and closing of the circuit breakers and caused substations to de- energize, and re-energize, affecting the balance of power in the grid. The malware was eventually able to shut down multiple substations in the transmission system. (Figure 3)

Immediate Effects

[16] Step-down substations lower the voltage so that distribution systems could deliver energy to homes and local buildings. In Massachusetts and Rhode Island, Accelerated Grid's substations worked in conjunction with the distribution system run by Light for All, making up a substantial portion of the grid. With the cascading effects of the malware on the transmission substations, over 1 million people in Massachusetts and Rhode Island were left without power. The malware also disabled any self-correcting or automatic mechanisms that could have normally helped to restart the systems. Data from the utility company's computers were deleted. Furthermore, a Connected Utilities substation also experienced major physical damage which was reported when smoke began appearing from one transformer, likely due to the increased pressure from the erratic behavior of the circuit breakers. (Figure 4)

[17] Immediately following the outage, local businesses and other infrastructure operations began facing serious complications as well. Critical institutions such as hospitals and government buildings had backup generators, but other industries that affected the greater public such as transportation, begin to suffer. In the Northeast, public transportation came to a momentary halt; the subway on the outskirts of Boston were delayed several hours, then came back with limited services using backup generators. Bus service was also impacted as traffic lights and signals switched to back up generators. The outage resulted in prolonged traffic, people having to walk places, and a surge in prices for ride share services. While there are no underground trains in the areas affected in Illinois and Indiana, buses experienced similar delays, leaving numerous people behind their daily schedules.

[18] Another area of concern was the water industry, given that electricity is needed for water plants that deliver clean and safe water to homes. Furthermore, even though backup generators exist in hospitals and other critical buildings, the water comes from outside sources and must be pumped through a system that both sanitizes and delivers water. The disruption in the energy delivery system created a problem for sanitation. Since electricity was cut off in both the Northeast and in the Midwest, millions of people were left without drinkable water. Plumbing also becomes a major concern, and people are forced to find different sources of water in order to use restrooms, showers, sinks and other systems.

[19] Furthermore, the outage also cut phone lines, and those without cell phones were unable to make calls. While longer term concerns included charging batteries for cell phones, those who were able to send messages or make calls were often unable to connect to their target person. Cell towers had backup generators but concerns about how long that would last also arose. This made it difficult for authorities to deliver critical information to people in a timely manner. There was no immediate information released regarding road closures or public transportation delays as well as possible accidents leaving people confused and anxious about safety. Updates on power restoration for the public were made, but how far they reached was uncertain.

Initial Response

[20] With response plans in place, the real time operators on site were instructed to attempt to restore power themselves. However, with the physical damage that occurred, the operators on scene struggled to do so. They were still under the impression that the damage came as a result of too much demand, or a natural cause, much like that of the Northeast Blackout of 2003, where transmission lines sagged into overgrown trees and caused a multiple day outage across the Northeast and Midwest of the country. Within a few hours, Accelerated Grid, Light for All, and Connected Utilities quickly exhausted their initial response mechanisms and managers knew that they need further assistance in order to recover. Each company had a different approach to their response and recovery.

[21] Accelerated Grid quickly received calls from customers about the blackout and reported that nothing out of the ordinary, such as a tree damaging a transmission line, occurred. Industrial control system experts from the company examined the issue. They were unable to trace the cause of the outage and or identify how the substations shut down so quickly. The employees at Accelerated Grid considered the list of possible causes, with cyber threat as an increasing possibility because all data from their computers had been wiped out. The in-house cyber employees were unable to get to the central location quickly. After five hours, their in-house employees arrived and completed their analysis of the systems. They were unable to isolate the malware. The company had not included a response for a data-wiping attack in their response plans and had no current backups for their control systems to help restore power. Their response plans indicated that they would reach out to CMA if something like this occurred, and CMA was contacted. CMA attempted to provide services but was unable to provide enough power to cover the entire outage area, citing distance, transportation, and concern about contaminating other systems with the malware as issues preventing a full-scale alternative energy source. As their response plan stated, the employees also decided to call the DHS fly-away team, who ensured that they would be given assistance as soon as possible.

[22] Light for All faced different circumstances than Accelerated Grid, as their systems were not directly infected by the malware. Since Light for All's distribution substations were directly connected to Accelerated Grid's transmission lines, they experienced an outage in delivery capability but had to wait for the transmission system to be fixed. In the meantime, their response plan for outages required them to reach out to their contracted industrial control experts at Stronger for You. The experts analyzed the effects of the malware on their part of the grid and found that no damage to the substations or lines had occurred. Their customers were without power, but Light for All had no options for using alternative sources to recover.

[23] In the Midwest, the situation was also different. Since Connected Utilities had limited in-house resources, they called their contractors. Since one substation that fed major distribution centers experienced major physical damage, the company's in-house operators were unsure of their next steps. The fire department had been called and the smoldering substation was no longer on fire. The operators attempted to get the power up and running, but due to the recent upgrades in their OT systems, the company did not have a backup transformer readily available. They had a plan to invest in one in the near future, but that was not going to help fix this emergency. They went through the steps outlined in their business continuity plans for restoring power but found that they are unable fix the failed systems. The employees began to consider other root causes for the failure in their control systems. After nearly six hours of analysis and forensics, they heard about the outage in the Northeast where a cyber-attack may possibly have been the cause. They contacted the Chicago office of CV1 for assistance, only to

learn that it would be another five hours before they could reach the site, due to added traffic from the outage. (Figure 5)

Transition to Recovery

First Steps

[24] After a few days, all three companies were able to restore power delivery, and the companies and the grid as a whole were on the road to recovery. Indestructor, the malware, wiped out most of its own footprint, but cyber vendors were able to analyze its effects and study how it was able to take down a major portion of the grid. Officials were called in, and the cause of the outage was released to the general public to assist others should similar issues be noticed.

[25] However, other long-term consequences of the attack were creating new concerns for the energy delivery companies. Top on the list were physical damage and future vulnerabilities. Executives at the three affected companies held emergency executive team meetings to identify resources necessary to avoid similar issues in the future and focused on the steps necessary to ensure that their systems were safe and protected. Working with their OT vendors, the ICS team and their cybersecurity peers removed the backdoor, and installed new authentication measures, patches, and software to decrease the system's vulnerability. Supply chain vendors were given new passwords and procedures for accessing ICS systems. To further prevent a reoccurrence in the future, executives from the energy delivery companies created an organization to make it easier to share information with each other about outages and recovery mechanisms to protect others from an event such as this one.

[26] The other industries impacted by this cyber-attack also had a difficult time recovering. The transportation across the four different states resumed normal services after three days, but the wake of their outage caused citizens and local governments to reexamine their own recovery and response mechanisms. Following this incident, the city transportation departments started brainstorming ways for their services to be more resilient. They planned on installing additional backup generators for power and established relationships with energy specialists should they need additional help. The water industry faced greater complications; without sanitary water, they were forced to create additional partnerships with nearby towns and states to get drinkable water to their citizens, which would be costly. It took a week for normal operations to resume and for the water plants to function properly, as there was heightened fear that the outage may have induced further damage. The communications sector gradually recovered as power was restored area by area. Telecom and cellular service companies also made plans to have additional backup power supplies and larger companies in

the areas of the outages considered plans for alternative telecommunications should their landlines and cell phones not work during an emergency situation.

[27] Luckily, few people were injured as a result of the power outage. Since hospitals had strong backup generators, critical patients were successfully cared for, and other urgent cases that occurred were diverted to hospitals that could accommodate them.

[28] While the local and state government buildings did not lose power, officials began thinking about damage to critical infrastructure and how to aid the utility companies next time. Topics of discussion ranged from establishing closer relationships with critical infrastructure companies, changing standards for response mechanisms, local coordinating boards to assist in emergency situations, review of regulations that might assist or inhibit response and recovery, and additional planning and response processes for officials.

Future Planning

[29] In the meantime, the ESCC decided to convene a meeting to discuss the Indestructor event, given that it was the first large-scale cyber-attack on an industrial control system in energy delivery subsector of the U.S. Even though the utility companies responded to and recovered from the attack, the ESCC believed that the process could have been more efficient and effective in practice. What could the ESCC do to assist utility companies, so this type of malware attack did not happen again? How could the ESCC assist utility companies of all sizes and capabilities with their cybersecurity response and recovery plans? Indestructor was an attack that impacted two different utility companies in geographically different regions at the same time. Resources were spread thin. Some expected resources were unable to assist in this situation, given the broad geographic impact. The ESCC begins to evaluate the likelihood that this would occur again.

[30] Their meeting led them to questions regarding response mechanisms in mitigating the attack that extend beyond a single, or even two companies. Since another large-scale attack could happen again, the ESCC focused on the ecosystem's response as a whole. They sought to answer one question: How can all companies be prepared for a cyber-attack? They decided that the response plans needed to include more detail, but what was the most appropriate mitigation plan?

FIGURE 1: OVERVIEW OF FICTIONAL UTILITY COMPANIES IN THIS CASE STUDY

Name	Locations Served	Description
Accelerated Grid	Greater Boston Area, mainly Southeast Massachusetts, Providence, RI	Transmission Company
Light for All	Greater Boston Area, mainly Southeast Massachusetts Providence RI	Distribution Company
Connected Utilities	Illinois and Indiana	Transmission and Distribution Company

FIGURE 2: RELATIONSHIPS BETWEEN UTILITY COMPANIES AND EXTERNAL SOURCES OF AID

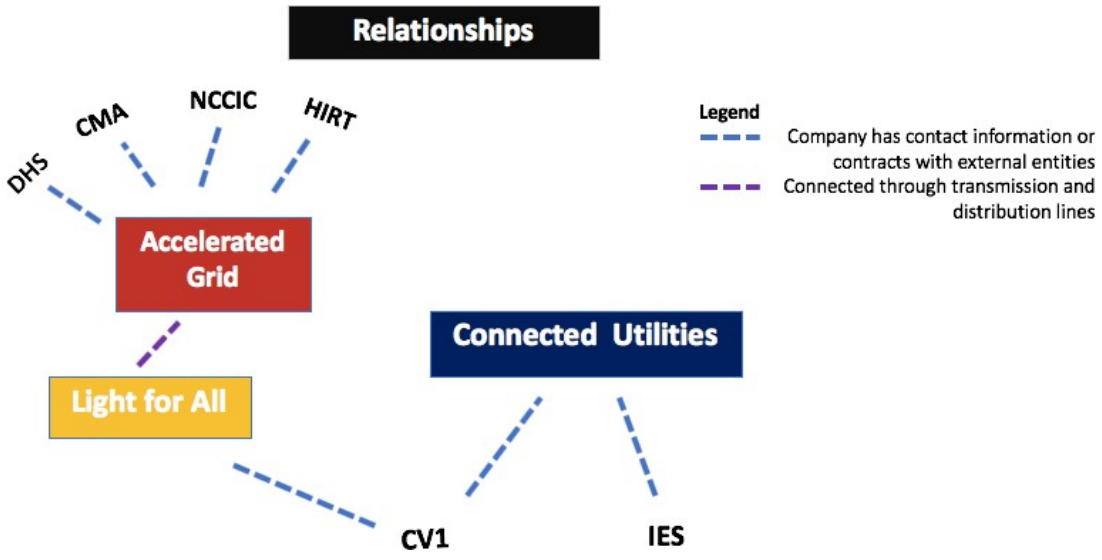

FIGURE 3: MALWARE ATTACK OUTCOME

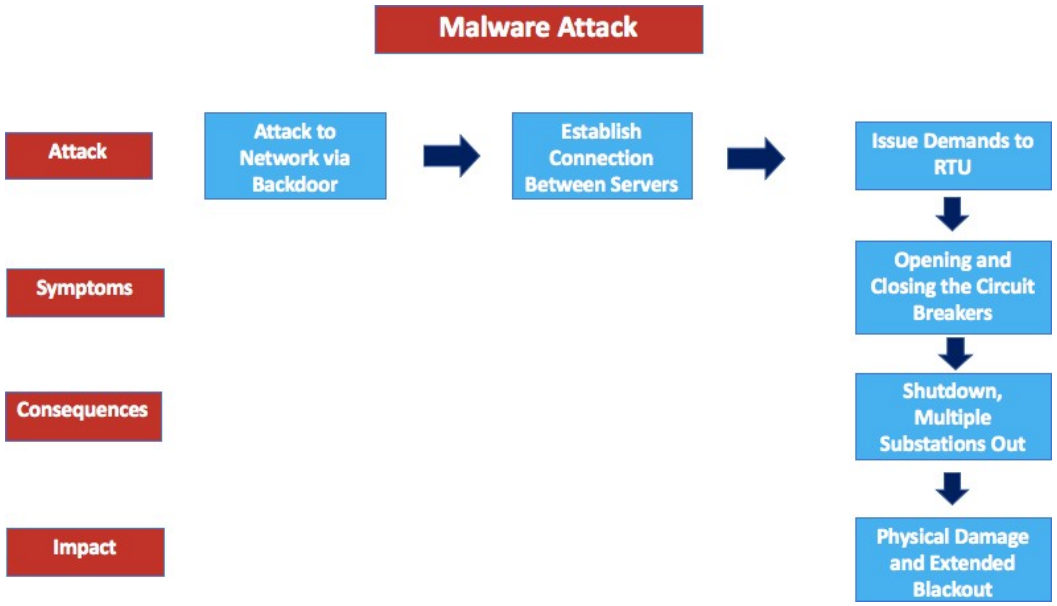

FIGURE 4: IMMEDIATE IMPACT ON ELECTRICITY GRID

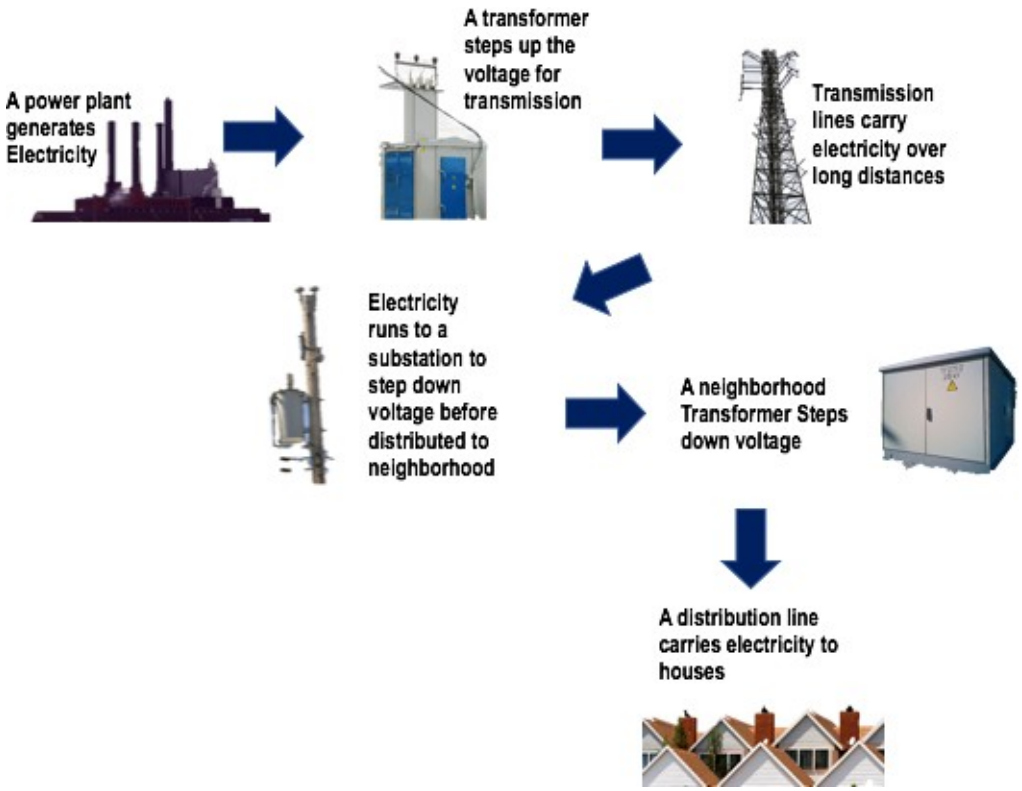

FIGURE 5: INITIAL RESPONSES BY COMPANIES TO MITIGATE ATTACK

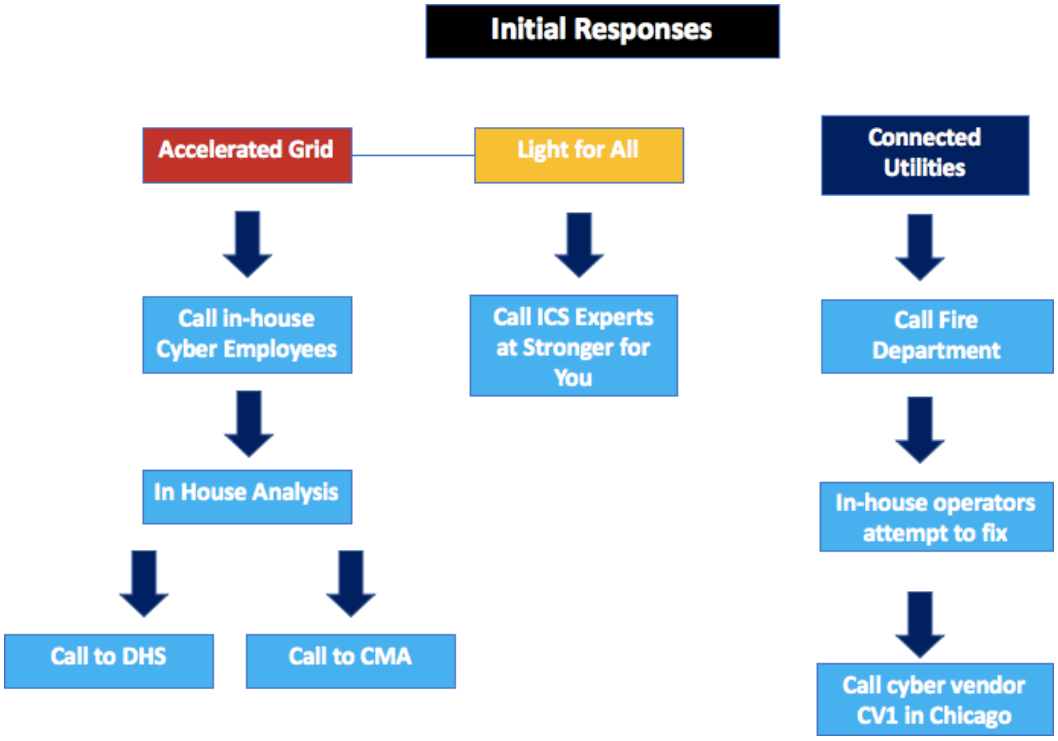

FIGURE 6: ACRONYMS USED IN CASE STUDY

Acronym	Full Name
IoT	Internet of Things
IT	Information Technology
OT	Operational Technology
MISO	Midcontinent Independent System
NERC CIP	North American Energy Reliability Corporation – Critical Infrastructure Protection
CMA	Cyber Mutual Assistance
ESCC	Electricity Subsector Coordinating Council
DHS	Department of Homeland Security
NCCIC	National Cybersecurity & Communications Integration Center
HIRT	Hunt & Incidence Response Team
ICS	Industrial Control System
RTU	Remote Terminal Unit
DNP3	Distributed Network Protocol 3
CV1	Cyber Vendor One
IES	Illinois Electric Systems