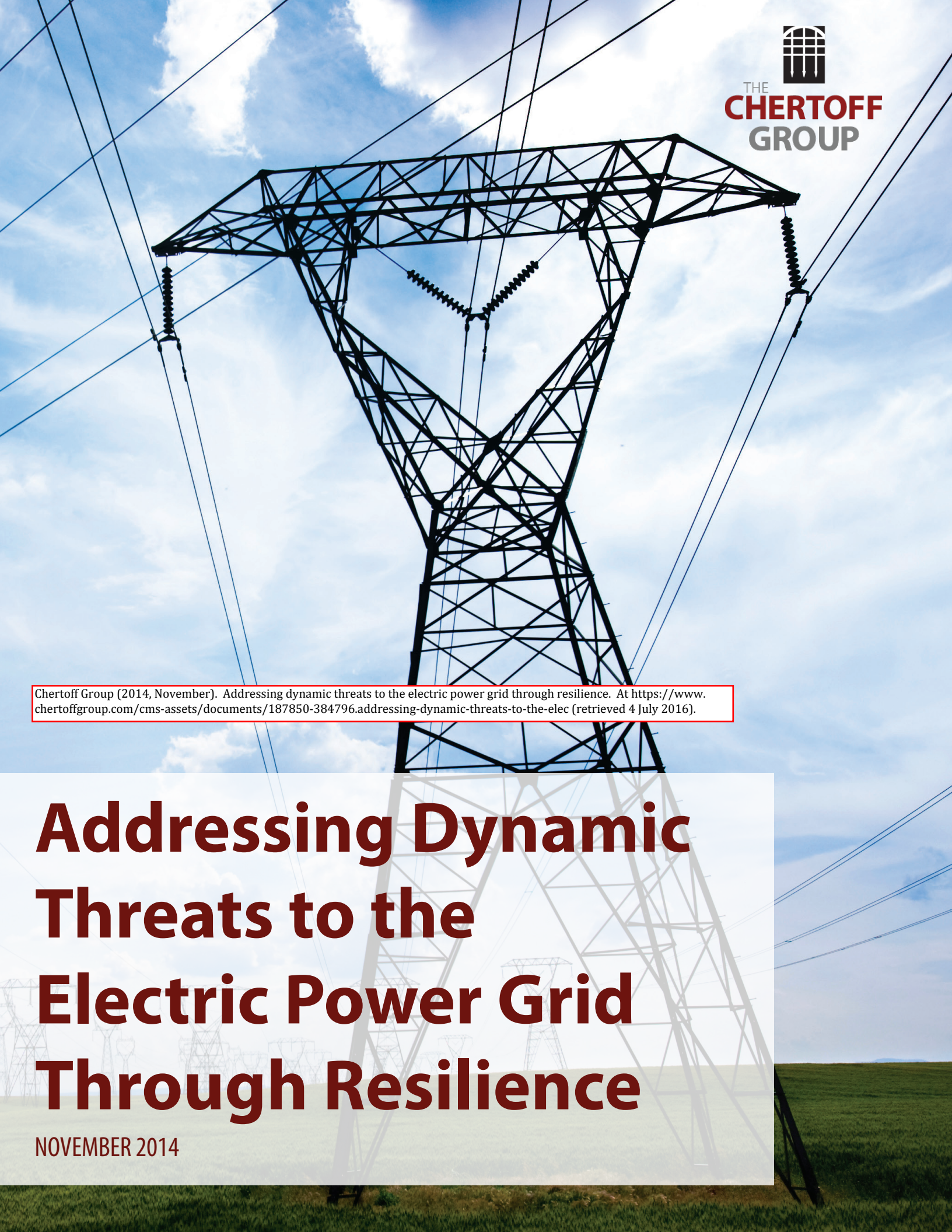


THE CHERTOFF GROUP

Chertoff Group (2014, November). Addressing dynamic threats to the electric power grid through resilience. At https://www.chertoffgroup.com/cms-assets/documents/187850-384796.addressing-dynamic-threats-to-the-elec (retrieved 4 July 2016).

Addressing Dynamic Threats to the Electric Power Grid Through Resilience

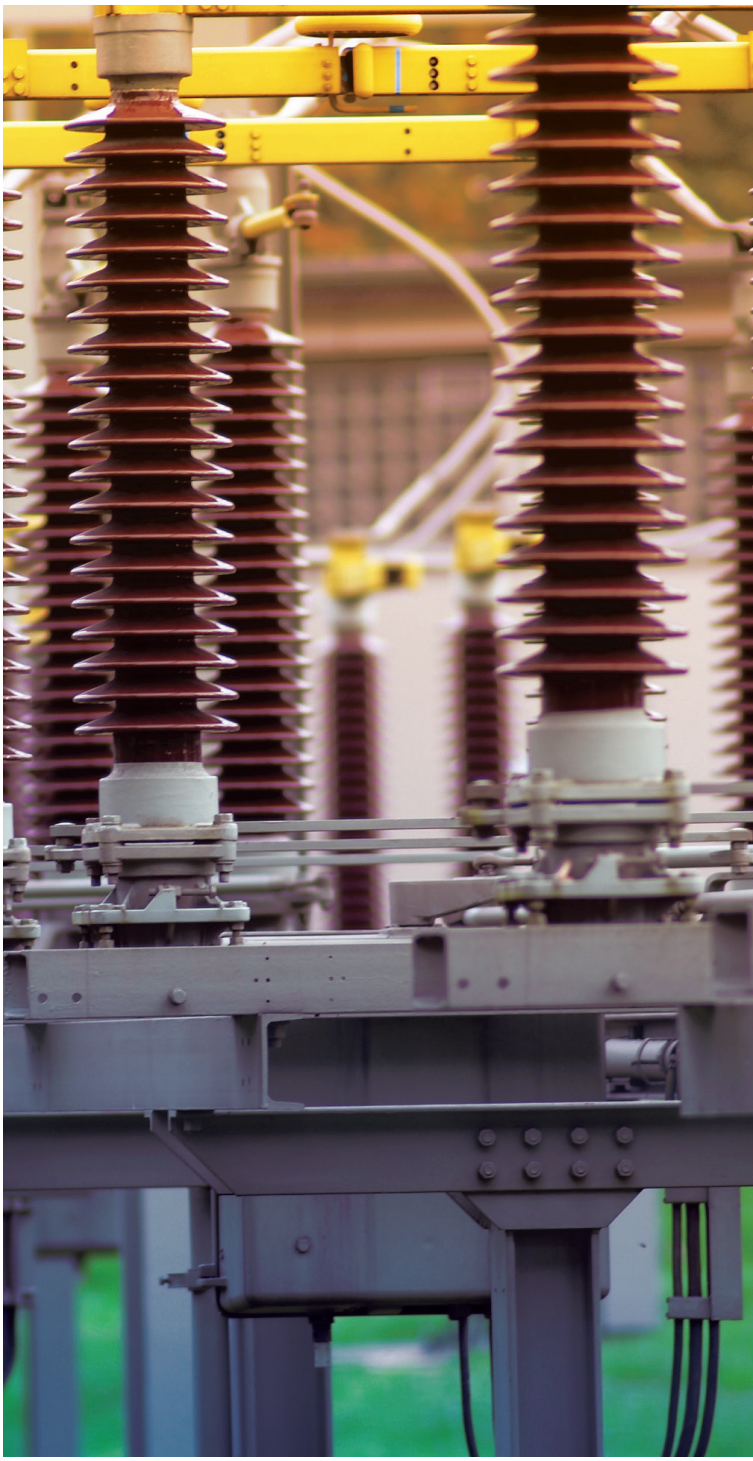
NOVEMBER 2014

INTRODUCTION

The U.S. electric power grid is an interconnected system made up of power generation, transmission, and distribution infrastructure. The grid comprises nearly 6,000 power stations and other small generation facilities; 45,000 substations connected by approximately 200,000 miles of transmission lines; and local distribution systems that move power to customers through overhead and underground cables.[1] Often called "the largest machine in the world," the U.S. electric power grid is considered "uniquely critical" [2] because it enables and supports other critical infrastructure sectors, including the oil and natural gas, water, transportation, telecommunications, and financial sectors. The use of electricity is ubiquitous across these critical infrastructure sectors, and our society's dependence on electricity continues to increase.

The electric power industry understands the critical service it provides and the impact that could result should the electric grid or the ability to deliver electricity be disrupted or damaged. The industry also recognizes that there is no single solution that can completely eliminate each and every risk to the grid. As a result, the industry works closely with government and other industry partners to apply an effective risk management approach focused on ensuring a reliable and resilient electric grid that can quickly recover and restore critical services to customers when power disruptions occur. This partnership informs necessary investments to better plan for and prevent highly consequential incidents and to strengthen capabilities to respond and recover quickly with minimal disruption or damage.

This report reviews the electric power industry's efforts to protect the grid and to protect against possible harm to our nation's power supply. It also recommends further initiatives that can help to strengthen and enhance resiliency.



MANAGING RISK
WITHIN A DYNAMIC THREAT ENVIRONMENT

By its nature, the electric grid is dispersed and includes potentially "soft targets," that are more easily identifiable targets due to its visible presence in communities across the nation. Due to this visibility and its extensive network, the grid may be viewed as vulnerable; however, the design of the grid is what actually makes it quite resilient. Redundancy is designed into the various components and systems of the electric power grid, which can limit potential damage from a variety of threats. Each power facility ranges in size, structure, and criticality. Many facilities are located in rural areas, open fields, and next to major highways and railroad tracks, while others are located in heavily populated areas.

When trying to determine the capabilities necessary to protect against current threats facing this diverse infrastructure—whether malicious attacks or naturally occurring events—electric companies must keep in mind that no enterprise or industry can eliminate risk completely. To be effective, critical infrastructure owners and operators must have a solid understanding of how to define security risk in order to effectively design plans that will minimize potential dangers.

Risk managers and power operators consider their analysis based on three variables:

(1) THREAT: the capability and intent to cause harm
(2) VULNERABILITY: the weaknesses or susceptibility that make harm possible, and
(3) CONSEQUENCE: the resulting types of harm

The standard risk equation for these three variables is expressed as:

The overall degree to which risk is measured manifests itself at the intersection of the potential capability and the intent to cause harm ***(the threat)***, the weaknesses that make harm possible ***(the vulnerability),*** and the resulting types of harm ***(the consequence)***. The likelihood of the threats is a function of the intent, capability, and motivation of each adversary in addition to the level of mitigation in place that adversary seeks to exploit.

INDUSTRY'S APPROACH
TO GRID SECURITY

Chertoff Group (2014, November). Addressing dynamic threats to the electric power grid through resilience. At https://www.chertoffgroup.com/cms-assets/documents/187850-384796.addressing-dynamic-threats-to-the-elec (retrieved 4 July 2016).

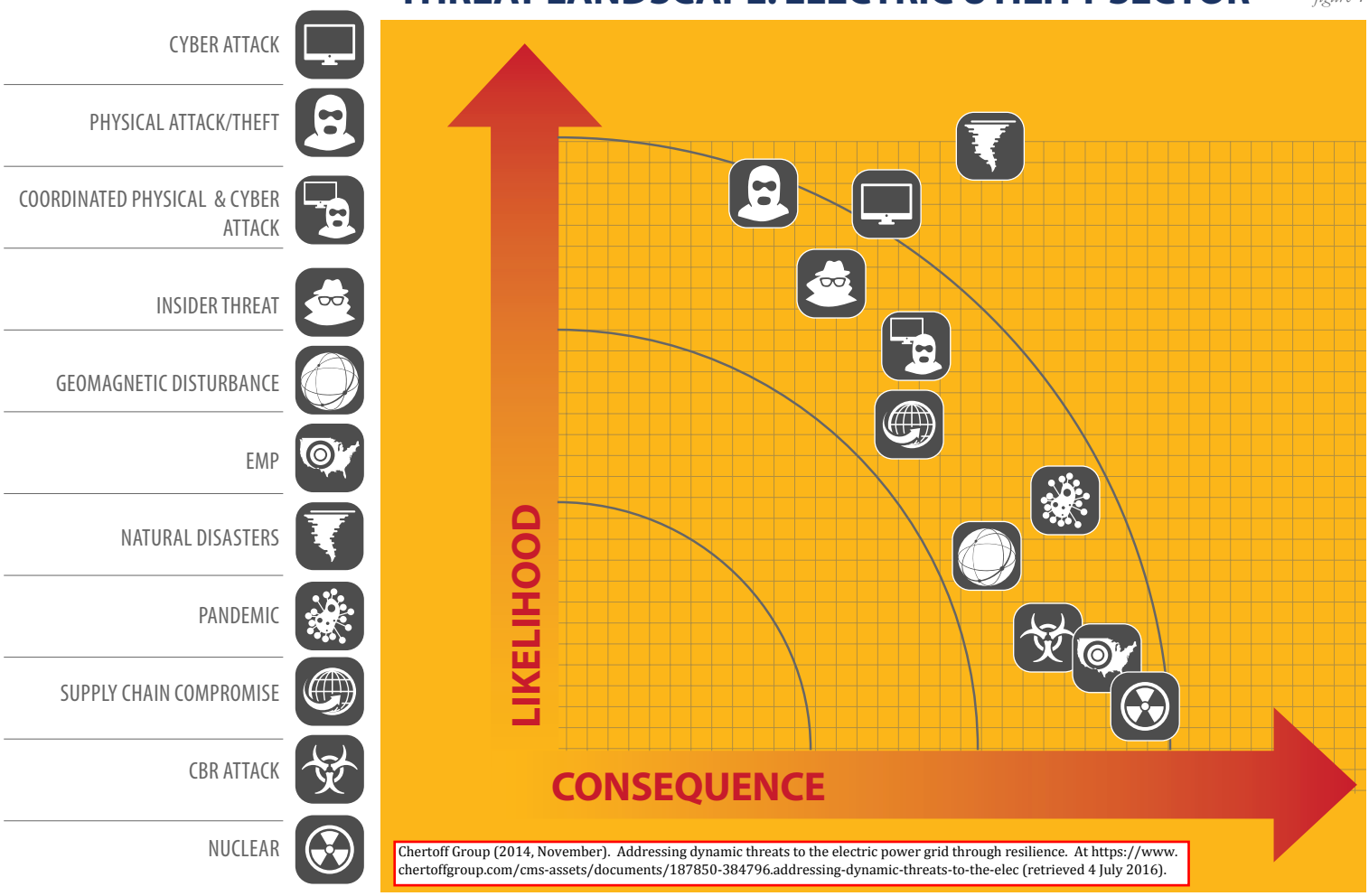
Today's threats to critical infrastructure range from incidents that are highly likely to occur, such as natural disasters and other weather-related events, to incidents less likely to occur, but with severe consequences, such as nuclear, chemical, biological, or radiological attacks. When fully considering this range of threats, the resulting consequences can vary significantly. Additionally, not all components of the grid are of equal criticality. Transmission infrastructure can be more critical than local distribution infrastructure, and the appropriate level of risk mitigation for each must take into consideration the likelihood and consequences of an incident. (See Figure 1.)

When considering the broad range of threats that could impact the Bulk Power System, electric companies recognize that any single security element or mitigation measure relied on can be defeated or can fail. Therefore, the industry strategically applies what is known as ***defense-in-depth***. Defense-in-depth is an approach to security that is characterized by the layering of security elements to successfully harden a target and mitigate its risk, especially during an attack. Through a layered approach of complementary elements, vulnerabilities can be mitigated and the impact of a negative event greatly reduced.

The defense-in-depth approach is successfully implemented across various industries, including government agencies and the military, to address both cybersecurity and physical threats. Within the electric power industry, the layering of security elements, as well as the creation of fault tolerant design, helps to prevent any single point of failure or wide-scale disruption of grid operations.

THREAT LANDSCAPE: ELECTRIC UTILITY SECTOR

figure 1



Chertoff Group (2014, November). Addressing dynamic threats to the electric power grid through resilience. At https://www.chertoffgroup.com/cms-assets/documents/187850-384796.addressing-dynamic-threats-to-the-elec (retrieved 4 July 2016).

INDUSTRY INITIATIVES

Protecting power grid infrastructure and supporting assets, which include physical assets, computer networks, and the control systems that support them, is a top priority for the electric power industry. The industry is proactively working through a variety of industry initiatives with a single goal in mind: strengthening the security, reliability, and resiliency of the electric power grid.

In 2011, the electric power industry sought to proactively and systematically identify threats that, if successful, would result in major consequences and interrupt companies' ability to generate, transmit, or distribute power. The ***Threat Scenario Project*** [3] described the top threat scenarios facing U.S. electric companies, the likely attack paths or target types, and the ways to mitigate or reduce possible areas of weakness or vulnerability. While not a comprehensive security risk analysis and assessment guide for each specific electric facility, the Threat Scenario Project helps electric companies quickly identify areas where security measures are sufficient and where gaps may exist, and begin the dialogue about additional measures that can be taken to help detect, protect against, respond to, and recover from a range of potential threat scenarios.

Another example of an initiative to ensure reliability of the grid is the industry's mutual assistance network, which is a voluntary partnership of electric companies from across the country committed to helping restore power following an emergency situation. This mutual assistance network provides an effective and coordinated effort to immediately mobilize assets and personnel needed to aid with the response and restoration of power under any circumstances.

Coordinated on a regional level through what are known as Regional Mutual Assistance Groups, electric companies request and receive line workers, tree cutting personnel, equipment, spare parts, and other forms of aid to restore critical power service to affected communities and customers.

The ***Spare Transformer Equipment Program (STEP)*** further illustrates the culture of mutual assistance created as part of the industry's business continuity and emergency planning efforts. During an event, the timely transportation of spare transformers is both critical and challenging. Very few means of transportation exist to carry transformers across the country safely and securely due to their size and weight. The program includes coordination for the transportation of transformers among the rail or barge and trucking sectors. With STEP, the industry has established a binding, contractual arrangement with participating companies to share critical assets in the event of long-term outages related to transmission transformers. STEP member companies currently conduct exercises on an annual basis to assess and improve the program.

To complement STEP, the industry developed the ***SpareConnect*** program, which provides an online tool for electric companies to network and share other related critical spare equipment, including bushings, fans, and auxiliary components in times of need. Investor-owned, municipal, and cooperative utilities are working to broaden membership into these important programs and to improve coordination with each other to further strengthen the industry's ability to respond quickly and to restore operations during emergency incidents.

> **"The electric power industry is proactively working through a variety of industry initiatives with a single goal in mind: creating a more reliable and resilient power grid."**

MANDATORY AND ENFORCEABLE
CYBERSECURITY STANDARDS

Because the electric grid provides such a critical service to the safety and security of our society, the electric power industry works closely with the North American Electric Reliability Corporation (NERC) and the U.S. government to coordinate efforts that can strengthen grid security against both physical and cybersecurity threats. As part of the Energy Policy Act of 2005 and the ongoing collaboration between industry and government, mandatory reliability standards were established to address the security of grid assets essential to the reliable operation of the electric grid. Known as Critical Infrastructure Protection (CIP) Standards, these standards are drafted by the industry and proposed by NERC and ultimately reviewed and approved by the Federal Energy Regulatory Commission (FERC).

To date, the electric power industry is the only critical infrastructure sector with mandatory, enforceable cybersecurity standards. Since 2008, the CIP standards have been updated as the threat and technology landscape continues to evolve.

Most recently, in March 2014, FERC directed NERC to take additional steps to address physical security risks and vulnerabilities to the most critical assets of the electric grid. [4] The industry and NERC worked together to provide a set of recommended measures that could be implemented across a diverse set of infrastructure and are adaptable to the evolving threat environment. Acting within weeks of FERC's directive, NERC filed the physical security standard (CIP-014) with FERC. FERC is expected to approve CIP-014 by the end of 2014.

These mandatory, enforceable standards serve an important role in creating a baseline for security. They require users, owners, and operators of the nation's electric grid to implement training, cyber and physical security measures, and response and recovery plans. Examples of these activities include, but are not limited to:

- identifying and categorizing critical assets;
- having security controls in place to protect assets or continue operations when faced with a compromise or intrusion;
- providing risk and security training for individuals with access to critical assets;
- ensuring incident response planning for unplanned events; and
- establishing recovery plans for business continuity and disaster recovery, which must be exercised annually.

To ensure compliance, NERC conducts rigorous audits around these standards. Entities found in violation face penalties of up to $1 million per violation per day.

> **"...mandatory and enforceable standards serve an important role in creating a baseline for security."**

VOLUNTARY CYBERSECURITY STANDARDS

The industry uses a number of voluntary standards and other best practices to protect the grid beyond the baseline security established by the mandatory and enforceable CIP standards. For example, in 2012, the electric power industry collaborated on a White House initiative led by the Department of Energy (DOE), in partnership with the Department of Homeland Security (DHS), to develop the ***Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*** to help measure and improve the industry's cyber readiness. The model helps electric companies and grid operators to assess their cybersecurity capabilities and prioritize their investments to enhance cybersecurity.

Also in 2012, electric power industry representatives assisted the National Institute of Standards and Technology (NIST), DOE, and NERC with the development of the ***Risk Management Process (RMP)*** guideline to help tailor cybersecurity risk management processes to meet organizational requirements. Companies can use the guideline to incorporate cybersecurity risk considerations into their existing corporate risk management processes.

In response to Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," [5] released in February 2013, the industry provided input to NIST and participated in workshops to develop the ***Cybersecurity Framework***. The industry collaborated with DOE to adapt this cross-sector framework to the existing standards and best practices (e.g., ES-C2M2) already in use by the industry.

BEYOND STANDARDS
INDUSTRY AND GOVERNMENT WORKING TOGETHER

Industry initiatives, coupled with both mandatory and voluntary standards, are only a portion of the industry's defense-in-depth approach to protecting the nation's power supply. Due to the critical role electricity provides, it is important to recognize that protecting the electric grid is a shared responsibility between the industry and the government. The government has a law enforcement responsibility and a national security mandate, while the industry owns most of the infrastructure and has the operational expertise.

To support this effort, the Electricity Subsector Coordinating Council (ESCC) was created. The ESCC serves as the principal liaison between the industry and DOE, DHS, FERC, the FBI, and the White House. The ESCC is focused on three key areas:

- Information Sharing
- Tools and Technology
- Incident Response

More specifically, the ESCC works with the government on preparing for, and responding to, those national-level incidents that could affect power grid operations. It is critical to proactively address the need for more robust information sharing, spare equipment requirements, incident response and recovery, and better ways to detect, identify and classify threats and vulnerabilities. Even more critical is the timely sharing of that information with industry peers, which is what makes for the most effective kind of industry-government partnership.

> **"The security of our nation's grid is part of a continuous dialogue between industry and senior government officials."**

The level of coordination among senior government officials and electric power sector executives is unprecedented. According to a recent report from the President's National Infrastructure Advisory Council, the electric power industry's CEO engagement with senior government officials is the model for other critical infrastructure sectors. [6]

A critical area of focus for the ESCC is information sharing and ensuring that important information flows throughout the industry in an efficient and timely manner. This increased sharing of information and close coordination among electric companies and the government enables the industry to detect, identify, and classify threats and vulnerabilities, as well as respond to, and recover from, incidents more effectively through pre-established relationships, protocols, and procedures.

The ***Electricity Sector Information Sharing and Analysis Center (ES-ISAC)*** establishes situational awareness, incident management, coordination, and communication capabilities within the industry through a timely, reliable, and secure information exchange. The ES-ISAC serves as the primary security communications channel for the electricity sector and enhances the industry's situational awareness to cyber and physical threats, vulnerabilities, and incidents.

Additional tools and technologies being applied throughout the industry also have bolstered situational awareness and information sharing. The ***Cyber Risk Information Sharing Program (CRISP)***, developed as a partnership between the DOE's Office of Electricity Delivery and Energy Reliability, the ES-ISAC, Pacific Northwest National Laboratory, Argonne National Laboratory, and participating electric companies, facilitates the timely sharing of cyber threat information and situational awareness tools to help inform important security decisions among participating companies. CRISP provides a near real-time capability enabling participating electric company owners and operators to voluntarily share cyber threat data to the government and receive machine-to-machine mitigation. The goal is to establish a sustainable program owned and operated by the private sector that enables near real-time data sharing and analysis. By the end of 2014, more than 20 of the nation's largest electric companies will be participating in the CRISP program.

BEYOND STANDARDS
INDUSTRY AND GOVERNMENT WORKING TOGETHER

> **"Increased sharing of information and close coordination among power companies and the government enables the industry to detect, identify, and classify threats and vulnerabilities…"**

Industry and government are working more closely together to strengthen planning procedures and response protocols established as part of the industry's emergency response plans. Efforts include: conducting classified threat briefings for CEOs to develop a better understanding of the threat environment; conducting education briefings to inform utility owners and operators, as well as law enforcement and other local stakeholders, about past incidents and resources available to further protect power grid assets; reviewing critical site security plans; and conducting more frequent exercises.

In November 2013, NERC conducted the second industry-wide grid security exercise, known as ***GridEx II***. GridEx II brought together more than 200 organizations and 2000 participants from industry, government agencies, and Bulk Power System partners in Canada and Mexico to participate. GridEx II also included an executive tabletop exercise that involved electric power sector executives and senior U.S. government officials, creating a robust exercise scenario that featured a combined physical and cyber attack as might be seen during a real-world event.

The GridEx II After-Action Report identified several recommendations derived from the exercise, including the need to adapt existing coordination and response mechanisms to a national scale and provide comprehensive situational awareness for crises similar to the "severe event" addressed in GridEx II. [7] GridEx II was a comprehensive security exercise with significant industry and government participation, and serves as an example of the commitment of stakeholders to continuously improve physical security and cybersecurity. NERC is already planning GridEx III, which is scheduled for the fall of 2015.

PUTTING STRATEGY TO THE TEST

As stated, the electric power industry's approach to risk management focuses on ways not only to prevent threats from causing harm or disruption to the power grid, but also on how best to respond and recover when an incident has occurred. Understanding how these plans and procedures are carried out in the real world can help to identify the success of their planning and where additional adjustments are necessary. Two recent examples illustrate the value of this risk management approach and how the industry has adapted to the realities of today's environment.

SUPERSTORM SANDY

In the fall of 2012, Superstorm Sandy presented extraordinary circumstances, delivering record storm surges across Connecticut, New Jersey, and New York, and storm force winds over an area 1,000 miles in diameter.[8] In addition, Sandy produced snowfall totals of up to 36 inches and blizzard-like conditions across the central Appalachians, especially in West Virginia and North Carolina.[9] More than 8.5 million customers were left without power,[10] making it the largest storm-related power restoration event on record. While storm recovery is not new for the industry, Superstorm Sandy was an unprecedented event within a heavily populated geographic region not accustomed to hurricanes. Emergency response plans and the mutual assistance network were activated before the storm's landfall with thousands of line workers, damage assessors, and tree removal personnel staged along the East Coast. With Superstorm Sandy impacting 24 states, the industry's mutual assistance network went beyond its typical regional requests for restoration personnel and requested assistance companies from as far away as Canada, Texas, and California to assist in the restoration effort.

METCALF SUBSTATION ATTACK

In the early morning hours of April 16, 2013, a physical attack occurred at Pacific Gas and Electric's (PG&E's) Metcalf transmission substation, located just south of San Jose, California. Two fiber-optic lines running underground near the substation were cut, and more than 100 rifle shots were fired at the substation's transformers. While substantial damage was done, not a single PG&E customer lost power. PG&E operators saw an anomaly in the system and rerouted power to another substation, which minimized the impact of the incident beyond the physical damage to the substation. While the circumstances of this specific event are both unusual and concerning, this event demonstrated the resiliency of the grid and the planning, training, monitoring, and response protocols of its operators.

Following the incident, PG&E voluntarily worked closely with law enforcement, including federal, state, and local authorities, and facilitated the flow of intelligence and threat information to educate and inform other grid operators across the United States and Canada about lessons learned as a result of this incident. PG&E also highlighted the available resources to help prevent similar attacks in the future. While there was substantial damage to the substation, the resiliency and the redundancy of the grid prevented a loss of power to a large portion of Silicon Valley.

Following every event, the industry comes together to identify best practices and areas for improvement. In these examples, training and continuous monitoring, emergency response protocols, as well as mutual assistance and aid during the events proved invaluable. However, these events also highlighted scenarios that require additional attention to ensuring lessons are learned and emergency preparedness efforts are strengthened.

Specifically, Superstorm Sandy brought increased urgency with regard to ensuring strong and effective communication during times of crisis. Activating mutual assistance programs and calling on additional resources when multiple states have lost power and require similar needs demonstrated the need for additional planning. Moving resources and power restoration assets across state lines to aid impacted areas required quick and coordinated cooperation among industry and government. As a result of the lessons learned from Sandy, the industry consolidated the number of Regional Mutual Assistance Groups from nine to seven, put in place a national framework to respond to an event of Sandy's size and scope, and formalized the role of the ESCC to be the primary liaison between the industry and government during an incident.

MOVING FORWARD

An effective risk management process requires constant review and assessment of the risk landscape, including the threats already described, as well as those the grid certainly will face in the future. In addition, risk management must take into account the evolving business and operational environment. For example, there are an increasing number of digital access points within the power grid that provide the potential for unauthorized remote access within the electric power industry's networks.

These examples can change the risk environment and require additional consideration when it comes to how the power grid is made more secure. While no one can know for certain what future events may include, there are measures that the industry and government can take today that will increase their ability to detect future threats and to apply appropriate measures to strengthen security while maintaining delivery of critical power services.

Recommendations for additional initiatives and investment include:

1. ENHANCE CROSS-SECTOR SECURITY COORDINATION AND AWARENESS

U.S. critical infrastructure is owned and operated by the private sector. Whether it involves transportation and delivery of electricity, cooling of power stations, or enabling the communication of critical operation functions, these critical services and operations have significant interdependency where each relies upon, and is responsible to, one another to ensure productive operations. As electric companies work to reduce vulnerabilities, bolster security, and enhance resiliency, they must consider their critical relationship and dependency with other critical infrastructure sectors, such as the transportation and telecommunications sectors, where they may face additional challenges should an incident occur. Sharing information, increasing situational awareness around threats and incident response, and conducting joint training and exercises with scenarios that realistically consider the possibility of failure beyond power loss will help to ensure more thoughtful preparation for future incidents.

MOVING FORWARD

2. ENHANCE SUPPLY CHAIN SECURITY STRATEGY

The disruption or compromise of the supply chain could have consequences for an electric company's ability to continue to operate at full capacity or to obtain the parts needed to recover from a significant incident. Products and services obtained through third-party providers are subject to both disruption and degradation of functionality or security that could be exploited by other adversaries and/or compromised by counterfeit materials. One goal should be to motivate and incentivize the investment in cybersecurity across the supply chain without encouraging overly strict rules and regulations that limit flexibility or make it too difficult to conduct business. Electric companies, in close coordination with suppliers and vendors, should develop a well-defined strategy that clearly outlines security measures and transportation requirements, as well as validation procedures to ensure these conditions are being met. This strategy would provide the necessary incentives to ensure a robust supply chain that meets today's security challenges.

3. RECRUITMENT, EDUCATION, AND TRAINING

Across both industry and government, there is a growing demand for new skills to ensure that workforce personnel operating critical infrastructure and key resources have the right experience and training to operate in a safe and secure manner. With increasing connectivity to the Internet and an infrastructure requiring information technology and operational upgrades, today's workforce needs to have the technical skills, as well as the cybersecurity expertise, to manage SCADA and industrial control systems, which provide critical command and control functions for the grid. The development of aggressive recruitment, education, and training programs to meet new technical challenges should be a priority for industry stakeholders, including the government.

4. CONDUCTING SPARE EQUIPMENT SHARING EXERCISES

For future exercises, planners and participants should incorporate the transportation of multiple spare transformers across one or more regions. Going forward, it is critical that industry be fully prepared to meet the logistical challenges of moving these transformers during or following a significant event.

5. CONTINUOUS MONITORING

Risk management through continuous monitoring allows for visibility of an organization's assets by leveraging data feeds to develop an operational picture of its security. This level of awareness and assessment of security controls allows an organization to counter the dynamic threat environment. In the past, organizations often have conducted security checks on an annual or quarterly basis in order to comply with a regulation or standard. In today's rapidly changing threat environment, continuous monitoring and assessment for physical and cyber threats is critical to understanding the health and behavior of the network and infrastructure at any given time. Continuous monitoring can help electric companies gain real-time visibility into their SCADA and industrial control systems, as well as the overall information technology and operational technology (IT/OT) environment enabling them to better detect, respond to, and recover from internal and external threats.

MOVING FORWARD

> **“While no one can know for certain what future events may include, there are measures that the industry and government can take today that will increase their ability to detect future threats…”**

6. INSIDER THREAT MITIGATION

Across many different sectors, incidents involving current or former employees, contractors, or other business partners are the most common, costly, and damaging type of security incidents. Of the more than 63,000 security incidents reported in Verizon's 2014 Data Breach Investigations Report, 18 percent were caused by internal actors acting either maliciously or carelessly.[11] In the Ponemon Institute's 2014 report on Privileged User Abuse & the Insider Threat, nearly half of the survey respondents (49 percent) representing a broad array of industry described their privileged user access policy, which can mitigate insider threats when effectively managed, as ad hoc.[12] Electric companies should consider comprehensive background checks and more frequent reviews of current employees who perform any critical service related to power grid operations to ensure they are able to identify potential insider threats before they occur. One layer that is essential to mitigating the insider threat is the constant review and determination of "need to know" and "least privilege" when considering who has access to critical business and operational functions within a utility. Without this constant review and determination, enterprises risk providing greater access than necessary to employees, contractors, and other partners, thereby greatly expanding points of vulnerability.

7. CONTINUE LOCAL LAW ENFORCEMENT COORDINATION AND EDUCATION

Building off of the industry's successful 2013-2014 physical security education campaign, electric companies can institutionalize their relationships with their respective local law enforcement. This relationship can help foster an increasing awareness of the threat, available resources, and communication around incident roles and responsibilities to ensure proper crisis management should an incident occur. Coordination with law enforcement is particularly crucial on the local level, where utilities can be proactive in developing working relationships with law enforcement and local field offices. Establishing regular meetings, conducting joint exercises, reviewing site security plans, and developing a better understanding of critical infrastructure security with law enforcement coordination will help create a more conducive security environment.

8. EXPAND CUSTOMER EDUCATION PROGRAMS ON SAFETY AND PREPAREDNESS TO INCLUDE SECURITY ISSUES

Electric companies play a unique and critical role in every community across America. Thus, it is vital customers understand how their electricity provider addresses cyber and physical security issues. Partnering with the government, companies should engage customers through town hall meetings, webinars, and social media campaigns to educate customers on their defense-in-depth strategies and emergency preparation and response plans. As companies have experienced with their ongoing efforts to educate customers on weather-related events, educating customers on security issues would go a long way in building stronger relationships and understanding if an incident occurs.

CONCLUSION

Grid security is a top priority for the electric power industry. Planning for and preventing potential attacks are critical to the economy and national security of the nation, as well as our way of life. The industry's approach to mitigating against today's threats requires a risk-based, defense-in-depth approach, because it is impossible to protect the electric grid from all threats. Industry practices a risk management approach that focuses on resiliency. Companies are focused on ensuring a reliable and resilient electric grid that can recover quickly and restore critical services to customers when power disruptions occur. Close coordination and collaboration with the government through the ESCC will help to strengthen the resilience and security of the electric grid further.

Planning and prevention strategies have strengthened the industry's capabilities to respond to and recover quickly from potential incidents and to minimize disruption and damage. In keeping with this defense-in-depth approach to security, the industry and the government must continue to look forward and consider further initiatives like those outlined in this report to enhance resiliency and adapt to the constantly evolving threat environment.

REFERENCES

1. U.S. Energy Information Administration, Annual Energy Outlook 2014, May 7 2014, available at: http://www.eia.gov/electricity/annual/html/epa_04_01.html; Federal Energy Regulatory Commission, Form 1 – Electric Utility Annually Report, 2013, available at: http://www.ferc.gov/docs-filing/forms/form-1/data.asp; Edison Electric Institute (EEI), Statistical Yearbook of the Electric Power Industry, 2014, available at: http://www.eei.org/resourcesandmedia/products/Pages/ProductDetails.aspx?prod=5A23A090-1104-4ADB-A828-FAC6D4FA3B62&type=Phttp://www.eei.org/issuesandpolicy/transmission/Pages/default.aspx

2. The White House, Office of the Press Secretary, Presidential Policy Directive-Critical Infrastructure Resilience, February 2013, available at: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

3. The Edison Electric Institute and The Chertoff Group, U.S. Electric Utilities: Top Threat Scenarios and Mitigation Actions, December 2011.

4. NERC, CIP Compliance, available at: http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/RD14-6.pdf

5. Federal Register, Executive Order 13636—Improving Critical Infrastructure Cybersecurity, available at: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

6. The National Infrastructure Advisory Council, Strengthening Regional Resilience, November 21, 2013, available at: http://www.dhs.gov/publication/national-infrastructure-advisory-council-strengthening-regional-resilience

7. NERC, Grid Security Exercise (GridEx II) After-Action Report: March 2014, available at: http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20After%20Action%20Report.pdf

8. U.S. Department of Commerce, National Oceanic and Atmospheric Administration (NOAA), Service Assessment: Hurricane/Post-Tropical Cyclone Sandy October 22–29, 2012, available at: http://www.nws.noaa.gov/os/assessments/pdfs/Sandy13.pdf

9. Ibid.

10. Ibid.

11. Verizon, 2014 Data Breach Investigations Report (DBIR), available at: http://www.verizonenterprise.com/DBIR/2014/

12. Ponemon Institute 2014 Report: Privileged User Abuse and the Insider Threat

About The Chertoff Group

The Chertoff Group is a premier global advisory firm focused exclusively on the security and risk management sector. The Chertoff Group helps clients grow and secure their enterprise through business strategy, risk management designed to protect against a broad array of threats and crises, and merger and acquisition services. The Chertoff Group, and its investment banking subsidiary Chertoff Capital, have advised on multiple M&A transactions totaling more than $6 billion in deal value. Headquartered in Washington D.C., the firm maintains offices in Austin, Houston, London, New York and San Francisco.

For more information about The Chertoff Group, visit
WWW.CHERTOFFGROUP.COM