

BUILDING A RESILIENT POWER GRID

Industry and government are working together to ensure necessary investments—not only to anticipate and prevent possible harm to critical energy supply—but also to ensure a constant focus on building a more resilient grid.

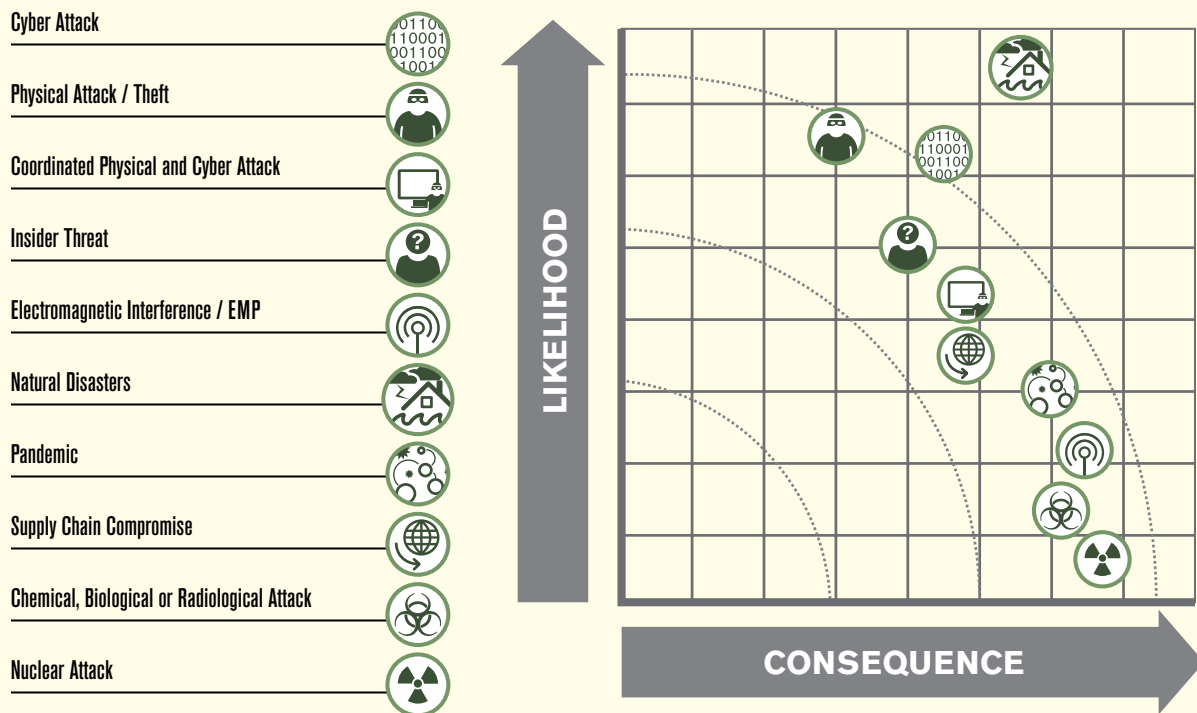
BY MICHAEL CHERTOFF

In the early morning hours of April 16, 2013, just 12 hours after the tragic Boston Marathon bombing, Pacific Gas and Electric's (PG&E's) Metcalf transmission substation, located just south of San Jose, CA, fell victim to well-planned and executed acts of sabotage. Two fiber-optic lines running underground near the substation were cut, and more than 100 rifle shots were fired at the substation's transformers and radiation cooling devices. While substantial damage was done, it is important to note that no power was lost. Why? PG&E operators saw an anomaly in the system and acted in accordance with their training by rerouting power to another substation. Their planning, training, monitoring, and response protocols helped them avoid a loss of power to a large portion of Silicon Valley.

There is no single solution that can completely eliminate each and every risk to our nation's power grid. However, the electric power industry and government can and are working together to ensure necessary investments—not only to anticipate, prepare for, and prevent possible harm to critical energy supply—but also to ensure a constant focus on building a more resilient grid.



FIGURE 1
THREAT LANDSCAPE: ELECTRIC POWER SECTOR



Source: The Chertoff Group, December 2013

Chertoff, Michael (2014, May). Building a resilient power grid. *Electric Perspectives* 39(3) 30-35: at [http://www.eei.org/resourcesandmedia/magazine/Issues/May-June%202014%20\(Vol.39%20No.3\).pdf](http://www.eei.org/resourcesandmedia/magazine/Issues/May-June%202014%20(Vol.39%20No.3).pdf) (retrieved 4 July 2016).

Spectrum of Threats

A significant step when building resiliency and an overall risk management strategy is to identify the range of threats that can impact operations at any given time. What are the risks that electric companies face today? Some might say it is the danger posed by nation states and global terrorism. Others might suggest cyber threats. Still others might point to natural disasters like earthquakes, tsunamis, or hurricanes. In fact, the principal risk many critical infrastructure owners and operators face is failure to take the proper steps to adequately identify each of these threats and plan accordingly.

In 2012, the Edison Electric Institute sought to proactively and systematically identify threats that, if successful, would result in major consequences and interrupt electric companies' ability to generate, transmit, and distribute power as they

do today. The Chertoff Group was pleased to share its knowledge and experience and to help the industry identify these threats. Known as the Threat Scenario Project, The Chertoff Group described the top threat scenarios facing U.S. electric companies, likely attack paths or target types, and further ways to mitigate or reduce possible areas of weakness or vulnerability.

More than 55,000 substations of 100-kilovolt capacity or greater exist as part of North America's bulk power system. Each of these facilities ranges in size, structure, and criticality. Some are located in rural areas and open fields. Others are located in heavily populated areas or even within buildings themselves. The one thing they have in common is that they all face a wide range of potential threats. (See Figure 1.)

As indicated, these threats range from those of high likelihood with significant consequences should they occur (such as natural disasters) to lesser likelihood with severe consequences (such as nuclear, chemical,

biological, or radiological attacks). As one reviews the Metcalf event and its implications, it is important to acknowledge that this is one of many threats the electric power industry must be prepared to address at any given time.

Effective Risk Management

Today, fundamental questions are being raised about how to protect critical infrastructure facilities and improve the ability to prevent, protect against, and respond to today's threats (both physical and cyber). For the electric power industry, there are important roles and responsibilities for both the private and the public sectors.

Electricity is a critical service to so many elements in our daily lives. It delivers power to our nation's critical military facilities, makes our hospitals operable, keeps our food fresh, allows our gas stations to operate, and keeps our lights on.

For this reason, the failure of one part of the network can have devastating collateral and cascading effects across a wide range of physical,

Michael Chertoff served as secretary of the U.S. Department of Homeland Security from 2005 to 2009. He is currently chairman and co-founder of The Chertoff Group, a global security advisory and risk management firm.


A significant step when building resiliency and an overall risk management strategy is to identify the range of threats that can impact operations at any given time.


economic, and social systems. Accordingly, government should have a role in security for those privately owned networks and systems, which are deemed critical infrastructure based on the interdependence or the essential nature of the services provided.

Ownership and control of these networks, such as electric companies, should remain in private hands, but government is a particularly important partner because it can leverage what former Defense Deputy Secretary William Lynn described in "Defending a New Domain: The Pentagon's Cyberstrategy" (*Foreign Affairs*, September/October 2010) as "government intelligence capabilities to provide highly specialized active defenses." In addition, should an emergency incident occur, clear lines of roles and responsibilities in the recovery process should be certainly understood, planned for, and frequently practiced.

How to Define Risk

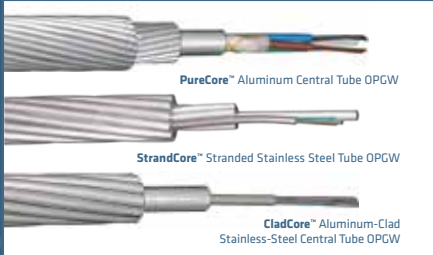
In order to make effective decisions when it comes to managing risk,





Announcing the Production of OPGW Cable in the USA

Prysmian Group is the world's leading supplier of both Power Cable and Optical Cable; allowing us to bring unique expertise to the OPGW marketplace. We have over 31 years' experience in OPGW cable design and production excellence. This expertise, combined with our industry leading manufacturing efficiencies, can provide you the highest quality and the most cost competitive solution available.



PureCore™ Aluminum Central Tube OPGW

StrandCore™ Stranded Stainless Steel Tube OPGW

CladCore™ Aluminum-Clad Stainless-Steel Central Tube OPGW

Manufacturing all aluminum and stainless steel OPGW designs.

For more information, please call 1-800-879-9862
 website: na.prysmiangroup.com/telecom email: comm.cables@prysmian.com

organizations should base their analyses on three variables: threat, vulnerability, and consequence. The overall degree to which risk is measured manifests at the intersection of a potential capability and intent to cause harm (threat), the resulting types of harm (consequence), and the weaknesses that make harm possible (vulnerability). These variables are not always equal, as some infrastructures may be more vulnerable than others, but the consequences may be relatively small. (See Figure 2.)

As true for mathematical equations of this form, if we are able to push any one of these elements to zero, then we can reduce our risk to zero. However, that is not possible unless we simply cease operations and the delivery of electric power as we know it today. In

order to apply an effective risk management strategy, one must consider all elements of the equation.

To date, most of the U.S. cyber protection and defense systems have focused on vulnerability. Common solutions and elements of an integrated physical and cyber defense plan may include building fences, installing alarms, or applying locks in a physical environment to building firewalls, implementing patches, applying system administrator controls, and exercising good cybersecurity habits also known as "cyber hygiene." All of these elements are focused on reducing vulnerabilities and preventing penetration.

Another element to understanding risk is consequence management. Here, a physical attack or cyber intrusion is presumed. It is not a matter of "if" but "when," and the focus is on how to continue operations despite being under attack. In the area of cyber, this is very true. Operating as if the attacker is already inside the network provides another layer of defense in the overall security

FIGURE 2
RISK FORMULA

$$\text{Risk} = \text{Threat (T)} \times \text{Vulnerability (V)} \times \text{Consequence (C)}$$

The Electricity Subsector Coordinating Council (ESCC)

strategy. The primary goal with consequence management is to minimize the potential impact of a security threat. This is the essence of resiliency.

Resiliency, of course, is the cornerstone upon which the electric power sector has built its ability to sustain operations in the face of today's threats. While most of us have only experienced the impact of natural disasters and the sector's ability to sustain operations and recover services moderately quickly, the same measures that work in storms, hurricanes, and blizzards will be those that apply in other threat scenarios as well.

As noted by Federal Energy Regulatory Commission (FERC) Acting Chairman Cheryl LaFleur in her recent letter announcing FERC's requirement for mandatory standards to protect critical grid facilities from physical security threats and vulnerabilities,

Together and individually, electric companies should continue to practice, test, and exercise their plans to ensure they are not only in place, but well-understood before a crisis occurs.

The ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure.

Areas of Focus:

Tools & Technology: Deploying proprietary government technologies on utility systems that enable machine-to-machine information sharing and improved situational awareness of threats to the grid;

Information Flow: Making sure actionable intelligence and threat indicators are communicated between the government and industry in a time-sensitive manner; and

Incident Response: Planning and exercising coordinated responses to an attack.

"...building a resilient grid requires a comprehensive and ongoing assessment of how the system is planned, constructed, operated, and secured under a range of conditions."

The electric power sector has for some time executed a range of activities consistent with a risk-managed approach that tries to reduce vulnerability as well as potential consequences. For example, electric companies that understand this need are working to apply a defense-in-depth strategy that attempts to eliminate any single point of failure and that requires an attacker to expend increasing resources to successfully penetrate the target. In addition, mutual assistance relationships exist across the industry, which enable the immediate sharing of resources—to include manpower as well as equipment—to quickly respond to and recover from a crisis event no matter where and when it occurs.

The Path Ahead

As we strive to improve risk management and reduction, not risk elimination, there are areas where we can continue to strengthen our capabilities.

First, industry and government must continue to build upon their senior-level engagement, through the Electricity Subsector Coordinating Council (ESCC), to plan and respond to national-level events. It is critical to leverage the resources that each brings to the ESCC, so that each benefits from information sharing about threats, where vulnerabilities exist, and how we can minimize the impact should a crisis occur with clear roles, responsibilities, and understanding of each other's actions. (See the sidebar, "The Electricity Subsector Coordinating Council.")

Second, we must continue to invest in education. Following the Metcalf incident in California, the Departments of Energy and Homeland Security, in coordination with the FBI, FERC, North American Electric Reliability Corporation (NERC), and electric sector partners conducted a series of briefings across the country for owners, operators, and local law enforcement regarding security of electric substations.

The goal of these briefings was to inform and educate these partners on not only tactical techniques used in this particular incident, but also the tools, resources, and best practices available to enhance information sharing, report suspicious behavior, and improve physical security and, of course, resilience. Cybersecurity is another area where everyone plays a role in helping to mitigate risk.

In November 2013, NERC conducted its second industry-wide grid security exercise. Known as GridEx II, this activity engaged more than 200 organizations and 2,000 individuals, including electric power sector CEOs and senior U.S.

government officials. Scenarios used in the exercise included a combined physical and cyber attack, posing critical questions for everyone involved about how the response and recovery to such an incident would take place. The GridEx II after-action report identified several recommendations derived from the exercise.

One of these recommendations highlights the need to adapt existing coordination and response mechanisms to scale and to provide comprehensive situational awareness for crises similar to the events addressed in the exercise. There is no doubt that these exercises bring tremendous value to all involved. Together and individually, electric companies should continue to practice, test, and exercise their plans to ensure they are not only in place, but well-understood before a crisis occurs.

The Metcalf incident has focused the electric power sector in terms of reassessing the wide range of threats it faces. For security discussions, this incident has become the current baseline for calibrating a physical threat to the sector. I expect, over time, the sophistication and resulting damage of the Metcalf attack will itself be exceeded and, eventually, a combination of a cyber and physical attack will take place.

In the end, risk management is not about responding to disasters after they occur. Of course, each incident should help to inform the strategy and lessons that should be learned.

However, managing risk is about looking ahead before the event occurs with the goal of preventing or reducing our vulnerabilities and consequences. By applying this strategy, our investment will be far less costly and could possibly prevent the crisis from arising in the first place. **EP**



Concrete Solutions from the StressCrete Group

With more than 50 years of experience in the industry, the StressCrete Group is North America's oldest and most reliable manufacturer of spun concrete poles. Concrete poles are ideal for utility and transmission distribution lines, offering the following benefits:

- Lifetime Warranty
- Zero Maintenance
- Easy Installation through Direct Embedment
- Quick Lead Times
- Three manufacturing facilities across North America
- Engineered to specifications
- Available in all heights up to 110 feet
- Environmentally Friendly

To request more information please phone toll free:

West & Midwest US: **1-800-837-1024**

South & Southeast US: **1-800-435-6563**

Northeast US & Canada: **1-800-268-7809**

or visit www.StressCreteGroup.com



King Luminaire • StressCrete • Est. 1953

STRESSCRETE GROUP

Quality People • Quality Products

Northport, Alabama • Jefferson, Ohio • Atchison, Kansas • Burlington, Ontario



Pegasus-Global

^ Zs/ ^ t WZKs/
 ◇ ž žh ž ◇ K - ž ž - ž ž Dž
 ◇ ž ž ž W ž . WW W ž W
 ◇ ž Z Z ◇ W W ž D
 ◇ ^ ž ž ' ž W ◇ ž ž ž ž ž W ž
 ◇ ž E E W Z ◇ ž ž D ž
 ◇ ^ ž Z

PEGASUS GLOBAL HOLDINGS, INC.

1750 EMERICK ROAD, CLE ELUM, WA 98922 • (509) 857-2235

WWW.PEGASUS-GLOBAL.COM