Lawyer Insights

The SAFETY Act: An Important Cyber Risk Mitigation Tool for Critical Infrastructure Companies

By Kevin W. Jones and Paul M. Tiao
Published in *Infrastructure*, ABA | October 25, 2019

Recent events highlight that critical infrastructure systems are prime targets for malicious actors seeking to use cyber and physical vulnerabilities to conduct potentially high-impact attacks or large-scale theft. Owners and operators of critical infrastructure face potentially substantial consequences in connection with cyber and physical security incidents. This article outlines a powerful resource available to help manage these risks: the Support Anti-Terrorism by Fostering Effective Technologies Act, or SAFETY Act.[1]

While cyber- and physical-security defensive measures have increased in recent years, so has the severity of the threat. The computerized, interconnected, and increasingly widely distributed nature of modern infrastructure and the systems used to operate it come with the risk of widespread, high-impact outages and other consequences from cyber or physical attacks.

A successful attack on critical infrastructure that results in a widespread and sustained disruption of service triggers government investigations and other inquiries into the companies at the center of the event. There is also a significant likelihood that impacted parties will bring lawsuits against those generally considered to be in a position to prevent such an attack. These risks cannot be completely avoided, so they must be managed.

Cyber insurance coverage is an important safeguard but not a complete solution to address the risk associated with an attack. While policies continue to evolve, they often contain significant exclusions to coverage. Furthermore, cyber insurance does little to address risks to a company's reputation.

The SAFETY Act provides a mechanism for critical infrastructure companies and their vendors to manage the potential consequences of a cyber or a physical attack. The SAFETY Act was enacted by Congress to encourage the development of antiterrorism technologies that protect the nation and its citizens. Obtaining SAFETY Act "designation" or "certification" provides significant statutory liability protections as well as substantial practical benefits that are discussed below.

The use of the SAFETY Act to manage liability risks has gained more attention in recent years, and some utilities have taken steps to obtain SAFETY Act coverage for their cyber and physical security programs. The following is an overview of the potential benefits of the SAFETY Act as well as the necessary criteria to receive SAFETY Act designation or certification.

The SAFETY Act: An Important Cyber Risk Mitigation Tool for Critical Infrastructure Companies
By Kevin W. Jones and Paul M. Tiao
Infrastructure, ABA | October 25, 2019

Critical Infrastructure Companies Confront Liability Risks from Cyber Events

There are significant liability risks for critical infrastructure companies and their officers and directors in the event of a widespread outage caused by a cyberattack. While the probability of a successful, large-scale attack remains low—largely due to increased vigilance among potential target companies—the potential impact of an attack remains high.

The Idaho National Laboratory prepared a report entitled Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, released in August 2016, that concluded that "[t]he likelihood for cyberattacks against utilities is increasing in frequency and severity of attacks."[2] A 2018 survey conducted by KPMG found that 48 percent of utility CEOs believe that a cyberattack on their company is inevitable.[3]

In December 2015, hackers managed to break into IT systems that operate large portions of the Ukrainian grid. They used that access to cause sustained electric outages for several hundred thousand people. In early 2016, ransomware attacks were reported against electric utilities in Michigan and Israel in which attackers attempted to take over utility computer systems and to interrupt key operations. In 2018, the Department of Homeland Security ("DHS") revealed that Russian hackers had infiltrated the control rooms of multiple electric utilities, gaining the ability to interrupt normal grid operations.[4] In early 2019, a major U.S. utility suffered a denial-of-service attack that interfered with grid operations. Though it did not result in customer outages, the attack was significant enough to warrant filing an electric disturbance report with the DOE.[5]

These attacks highlight the fact that critical infrastructure remains vulnerable and that attackers seeking to make an impact are likely to target utilities, given their critical role in modern life.

Although utilities enjoy certain common law and tariff protections against liability from outages caused by cyber or physical attack, those protections evolved in an earlier era, when the threat of widespread outages resulting from terrorist attacks was not a consideration. It is unclear to what extent those protections can be relied upon to defend against claims arising from a catastrophic outage due to an inadequate cybersecurity program. Historically, where there is a significant outage, traditional tariff and common law liability protections have been subject to challenge. In major outages during the past 40 years, utilities have often been subject to some degree of liability in spite of common law and tariff protections.[6] Deregulation of some infrastructure functions has further eroded those historic liability protections.

A utility suffering from a cyberattack that causes a widespread outage could spend years defending the resulting litigation. The utility or its insurer likely will pay some form of damages, through either a court award or a settlement. To the extent that the products or services of a vendor are implicated in the cyberattack and outage, the vendor is less protected by traditional liability limitations and therefore bears even greater risk of liability.

In addition to claims against the company and its vendors, the directors and officers of these companies can be targeted with a variety of claims. The potential allegations range from failing to adequately protect the company or its customers against a cyberattack to failing to make adequate disclosures about the state of the company's cybersecurity practices. DHS certification may provide a powerful defense to claims of inadequate Board oversight of security risks. Lawsuits of this nature

otherwise can be time-consuming, distracting, and expensive to defend. In addition, as with outage liability claims, resolution of these lawsuits often results in substantial payments by the target company, its directors and officers, or their insurers.

Although various industry standards have led to more stringent cyber and physical security practices, they have also elevated the potential liability risks associated with a major attack because they establish defined standards against which to measure a utility's preparedness measures. This risk is heightened by the fact that when a widespread outage occurs, regulators tend to conduct investigations, many of which are disposed of through settlements where there is a finding of one or more reliability standards violations. Such violations can serve as evidence or even a per se finding of negligence or gross negligence on the part of the utility.

SAFETY Act Provides Substantial Liability Protections

In conjunction with appropriate cyber insurance, coverage of a critical infrastructure company's cyber and physical security programs under the SAFETY Act can substantially mitigate liability risks from cyber or physical attacks.

The SAFETY Act was enacted as part of the broader Homeland Security Act of 2002 to help facilitate the development and deployment of antiterrorism products and services (referred to in the statute as "technologies") by granting various liability protections to companies that develop such products and services. The SAFETY Act offers covered technologies various protections against third-party liability for injury, loss of life, or damage to property or businesses arising out of an act of terrorism in circumstances where the applicable technology is deployed in defense against, or in response to, such an act. An "act of terrorism" is defined as any act determined by the Secretary of Homeland Secretary to have (i) been unlawful; (ii) caused harm to a person, property, or entity, in the United States, or in the case of a domestic U.S. air carrier or a U.S.-flag vessel, in or outside the United States; and (iii) used or attempted to use instrumentalities, weapons, or other methods designed or intended to cause mass destruction, injury, or other loss to U.S. citizens or institutions.

The SAFETY Act Application Process

DHS's Office of SAFETY Act Implementation (OSAI) is responsible for administering the SAFETY Act. OSAI's SAFETY Act implementation regulations provide increasing levels of protection, and corresponding review and evaluation, for covered technologies through "designation" and "certification." These SAFETY Act protections are obtained through an application process. OSAI assesses such applications according to a number of statutory criteria, including large or unquantifiable potential third-party liability risk exposure; likelihood that without the SAFETY Act's protections, the liability associated with the product or service would prevent or curtail its deployment; potentially substantial risk exposure to the public should the product or service not be deployed; and any other factors DHS deems relevant to U.S. security.

Designation requires that applicants demonstrate through these criteria that the technology shows effectiveness with confidence of repeatability. Certification additionally requires that the applicant show a high confidence of repeatability. This is established by not only satisfying the requirements of designation but also meeting three additional criteria: (i) the technology performs as intended, (ii) the technology conforms to specifications, and (iii) the technology is safe for use.

For a technology that has been granted designation, third-party liability for damages arising out of an act of terrorism is capped at the level of the applicant's required insurance coverage, which is determined by OSAI as part of the application process. Designation also carries with it a series of additional risk-mitigation measures, including exclusive jurisdiction in federal court for all lawsuits, a bar against punitive damages and prejudgment interest, a limitation on noneconomic damages, and liability only in proportion to the responsibility of the seller of the technology.

Certification provides the same protections as those provided by designation but also provides more complete liability protection by allowing the seller of the covered technology to assert the government contractor defense (a broad defense that forecloses most claims). The government contractor defense may be rebutted only by proving with clear and convincing evidence that fraud or willful misconduct occurred by the seller in submitting information to DHS.

Each designated or certified technology is listed as an "approved product for homeland security" on the DHS website unless the applicant requests to keep this information confidential. Sellers of designated or certified technologies are also authorized to affix the DHS SAFETY Act "seal of approval" on their product.

In addition, the Act provides that the only proper party defendant to a lawsuit arising from an act of terrorism is the technology's seller. Thus, customers, clients, subcontractors, and vendors that either use the technology or support the seller in deploying the technology are immune from liability.

Under the SAFETY Act, OSAI has 120 days from the completion of an application to render a decision. A grant of designation or certification is good for five years, after which the company must reapply for SAFETY Act coverage.

Critical Infrastructure Providers Can Benefit from the SAFETY Act

Since the SAFETY Act's passage, DHS has recognized protections for an increasingly broad array of technologies. While many covered technologies are specific equipment, devices, computer programs, and similarly discrete and specific assets, the SAFETY Act definition of covered technologies is not so limited. A "Qualified Anti-Terrorism Technology" is defined in the statute to include any "product, equipment, service (including support services), device or technology (including information technology) designed, developed, modified or procured for the specific purpose of preventing, detecting, identifying or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary (of Homeland Security)."[7]

The inclusion of the term "services" and "support services" within this definition is significant because it means that SAFETY Act coverage can be extended to not only equipment and applications but also security processes and procedures, including those a company develops for its own purposes. OASI has awarded SAFETY Act coverage to service providers, both to third-party sellers of security services as well as to entities that develop their own internal security programs.

OSAI is now working to extend SAFETY Act protections to critical infrastructure companies' internal cyber and physical security programs. In conjunction with the National Institute for

Standards and Technology's development of the Cybersecurity Framework and the Department of Energy's Cybersecurity Capability Maturity Model (C2M2), OSAI has issued guidelines to critical infrastructure owners and operators to seek coverage for part or all of their internal cybersecurity programs.

The SAFETY Act, therefore, provides an important avenue for critical infrastructure companies to mitigate potential liability resulting from a cyber or physical attack by obtaining designation or certification for internal cyber and physical security programs and processes. DHS has now granted this kind of enterprise-wide coverage to critical infrastructure companies under the SAFETY Act, and more companies are in the process of seeking protection through applications for designation or certification.

For an infrastructure company to obtain SAFETY Act coverage for its entire program, it must show OSAI that all aspects of its cybersecurity program, from identification of critical cyber assets and other protected cyber assets to protection mechanisms and recovery and restoration plans, satisfy the stringent criteria for designation and certification.

Practical Benefits of SAFETY Act Designation and Certification

In addition to the powerful statutory protections outlined above, SAFETY Act designation or certification provides significant practical benefits to owners and operators of critical infrastructure. Even in the absence of a declared act of terrorism, SAFETY Act designation or certification provides a compelling "seal of approval" from the DHS that is easily communicated to key constituencies and audiences both before and after a cyberattack.

Having a company's cyber or physical security program awarded a SAFETY Act designation or certification and deemed an "Approved Product for Homeland Security" provides an effective and concise validation of the strength of the company's internal programs. This can be valuable in interactions with regulators and other government officials, investors, consumer representatives, and other important constituencies. Furthermore, in the event of a cyber or physical incident—even if not declared to be an act of terrorism—SAFETY Act designation or certification provides compelling evidence of the company's diligence in developing and implementing appropriate defensive measures in accordance with applicable standards and prevailing best practices. This can have substantial reputational benefits both before and after an incident and can significantly mitigate liability risks.

In addition to these benefits, SAFETY Act designation or certification provides an independent demonstration to underwriters that a utility is managing risk effectively. This has the potential to improve the scope of insurance coverage available to the company and reduce the cost of that coverage.

Conclusion

Threats to critical infrastructure from malicious actors have increased significantly in recent years. From financially motivated ransomware attacks to geopolitically motivated attempts to disrupt system operations, these threats present the potential for significant liability on the part of companies that own and operate critical infrastructure as well as on the part of their directors and officers. The SAFETY Act represents an important tool to help manage these risks.

The SAFETY Act: An Important Cyber Risk Mitigation Tool for Critical Infrastructure Companies
By Kevin W. Jones and Paul M. Tiao
Infrastructure, ABA | October 25, 2019

In addition to powerful statutory protections that come with SAFETY Act designation or certification, the program provides meaningful practical benefits. These flow from the extensive review and independent validation of the strength of a company's physical or cybersecurity programs. This DHS "seal of approval" can be highly effective in interactions with regulators and other government officials, shareholders, customers, and other important public relations constituencies. It may also provide a meaningful benefit when negotiating insurance coverage and premiums.

Notes

1. Pub. L. No. 107 296, 116 Stat. 2135 (2002), codified at 6 U.S.C. §§ 441 444.

2. MISSION SUPPORT CTR., IDAHO NAT'L LAB., CYBER THREAT AND VULNERABILITY ANALYSIS OF THE U.S. ELECTRIC
SECTOR (Aug. 2016).

3. KPMG, 2018 KPMG CEO OUTLOOK: POWER & UTILITIES (Nov. 14, 2018).

4. Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, WALL ST. J., July 23, 2018.

5. Blake Sobczak, "Cyber Event" Disrupted U.S. Grid Networks—DOE, ENERGYWIRE, Apr. 30, 2019.

6. Paul M. Tiao & Brian M. Zimmet, Using the Law to Your Advantage, POWERGRID INT'L. Excerpt originally published as SAFETY Act Helps Manage High-Impact Cyber and Physical Security Events, ELEC. LIGHT & POWER, Feb. 22, 2017.

7. 6 U.S. Code § 444(1).

Paul M. Tiao *is a partner in the Washington, DC office, and founder and co-chair of the firm's Energy Sector Security Team. With experience in government and the private sector, Paul brings in-depth knowledge of cyber and physical security, internal investigations, law enforcement and national security to every client matter. He can be reached at +1 202 955 1618 or ptiao@HuntonAK.com.*

Kevin W. Jones *is a partner on the Energy and Infrastructure Team in the New York, NY office. Kevin's practice focuses on regulatory and market design matters for electric sector clients. He can be reached at +1 212 309 1188 or kjones@HuntonAK.com.*