Chicago Daily Law Bulletin.

Serving the city's law profession since 1854

January 11, 2016

Cybersecurity: Just how safe is U.S. electricity grid?

By Daniel A. Cotter
Dan Cotter is a partner at Butler, Rubin, Saltarelli & Boyd LLP and an adjunct professor at The John Marshall Law School, where he teaches SCOTUS Judicial Biographies. He is also immediate past president of The Chicago Bar Association. The article contains his opinions and is not to be attributed to anyone else. He can be reached at dcotter@butlerrubin.com.

Lawyers who have attended any substantive conference in the last 18 months have likely heard at least one update on cybersecurity, a topic that has garnered much attention as well-publicized hacks of private and public sector organizations continue to grow in frequency and severity.

Late last year, at least two publications focused on the threats cyberattacks present to the United States power grid as well as the losses and issues potentially triggered by such attacks. This column summarizes two of those publications.

Lights out

In October 2015, longtime "Nightline" anchor Ted Koppel published his book, "Lights Out." The book analyzes the threat of a major cyberattack to the power grid and the blackout and chaos that might ensue. Koppel organized the book into three parts: 1) A Cyberattack, 2) A Nation Unprepared and 3) Surviving the Aftermath. Part 1 focuses on the vulnerability of the power grid and describes how such an attack might occur.

Koppel opens Chapter 2 of Part 1 with a sniper attack that occurred in 2013 at Pacific Gas and Electric Co.'s Metcalf Transmission Substation in San Jose, Calif. The well-planned attack was widely reported by The Wall Street Journal and has never been solved.

The attackers knocked out 17 giant transformers using AK-47 assault rifles, causing significant damage that took 27 days to fully remediate, but power grid officials were able to avoid a blackout by rerouting power supplies. Koppel also addresses electromagnetic pulse (EMP) attacks.

EMP attacks are acts in which nuclear-armed missiles are launched and exploded at high altitudes over a nation. The result of an EMP attack is the destruction of electronic equipment, including that used in our power grid, over a wide area or region.

Koppel interviewed a number of former government executives, including Richard A. Clarke, former national coordinator for security, infrastructure protection, and counterterrorism, to gauge our government's readiness and preparation for a cyberattack.

Clarke notes that the interconnectedness of our grid has led to a major vulnerability. Currently, "almost all operational phases of thousands of power companies are interconnected" and use "the same supervisory control and data acquisition (SCADA) systems."

Anywhere in the world, the SCADA systems are the same. Craig Fugate, administrator of the Federal Emergency Management Agency, worries that someone with knowledge of the SCADA system could "engineer 'a series of events that seem totally unrelated' but which could … 'turn the lights out very quickly over large areas.'"

Part 1 questions what the odds of a major cyberattack on the United States power grid might be. While providing no answers, Koppel concludes this chapter by stating, "the insurance industry won't bet against it" after a discussion with Ajit Jain, CEO of the Berkshire Hathaway Reinsurance Group.

Part 2 of the book addresses the challenges if an attack were to occur and portrays the United States as unprepared for an attack of any magnitude. Koppel notes that the transformers are expensive, that most are built overseas and that each transformer weighs 400,000 to 600,000 pounds. Transportation of these transformers would require use of a specialized railroad freight car and, because many of these transformers were delivered 40 or more years ago, many of the rail lines necessary to transport them no longer exist.

The remainder of Part 2 portrays the various federal agencies that might be called upon to address such a cyberattack as uncoordinated and overconfident in the ability of our nation to respond to such an attack.

Koppel focuses on how some communities in Wyoming, have developed some self-resiliency, referring to these people as "preppers." Preppers have built shelters and homes that would shelter the inhabitants reliably, are energy self-reliant and have stored supplies, food, water and munitions that would enable the preppers to survive for extended periods of time should the power grid go down.

Koppel also focuses on Mormonism and its tenets regarding preparation for catastrophes as guidance for our consideration.

Business blackout

The second publication referenced is a report, "Business Blackout: The Insurance Implications of a Cyberattack on the US Power Grid," published by Lloyd's and the University of Cambridge Centre for Risk Studies.

Lloyd's makes clear in its opening disclaimer that it "does not predict any catastrophes." "Business Blackout" addresses the potential for a cyberattack on the United States power grid through the prism of insurance exposure and risk, noting that "cyber is an underinsured risk."

Lloyd's portrays a "hypothetical scenario of an electricity blackout that plunges 15 states and Washington, D.C., into darkness and leaves 93 million people without power," which it refers to

in the report as the Erebos Cyber Blackout Scenario. The Lloyd's report states that the Erebos Cyber Blackout Scenario is "improbable, [but] technologically possible" and within the 1:200 benchmark return period that insurers must take into account.

Lloyd's identifies six primary categories of insurance claimants that would result from such a blackout: 1) power generation companies; 2) defendant companies (sued by the power generation companies); 3) companies that lose power; 4) companies indirectly affected (supply chain disruption); 5) homeowners; and, 6) specialty (such as event cancellations).

The Erebos Cyber Blackout Scenario is initiated by an unidentified group that hires a number of "morally dubious programmers" who individually have little idea of the ultimate overarching goal. These programmers — hackers — penetrate the security layer on the power grid.

The installed malware remains dormant for some time and then is activated. More than 70 generators are infected across the grid. The blackout occurs when damage to more than 50 generators is inflicted by the malware installed by the hackers. Most of the generators can be repaired, and power is restored within three days, but some areas remain affected for up to two weeks.

Lloyd's then assesses the primary effects of the blackout. These include: a) general health and safety, b) productivity losses, c) trade impacts, d) consumption spikes, e) water supply issues, f) transportation impacts, g) communication limitations, and h) tourism reductions.

The Lloyd's report also identifies a number of secondary effects and long-term effects. Under three blackout scenarios (S1 and S2, for standard variant, and X1, for extreme), Lloyd's estimates the total economic cost of the Erebos Cyber Blackout Scenario from $60.9 billion under the S1 scenario to $222.83 billion under the X1 scenario. Lloyd's breaks down those estimates by sector at Table 3.

Lloyd's then turns to cyber as an insurance risk, noting that "cyber insurance is a rapidly growing market." The report notes that information technology cyber risks are addressed by the current cyber insurance market, but operational technology attacks, "such as an attack on a manufacturing plant," are not very common and coverage for such attacks is not prevalent in the cyber insurance market.

The Lloyd's report identifies by type of insurance claimant the coverages that might be implicated by an event such as the Erebos Cyber Blackout Scenario. The coverages include property damage, business interruption and contingent business interruption.

Applying the various effects and forms of coverage by claimant type, the Lloyd's report at Table 5 provides an estimate of the insurance industry's losses resulting from the three scenarios referenced above. Using this format, Lloyd's estimates the insurance industry losses from a low of $21.4 billion to a high of $71.1 billion.

The report also identifies some areas of insured losses not addressed by the estimates. Lloyd's notes, "No attempt has been made to apportion losses between primary insurers and their reinsurers."

Lloyds concludes its report by reiterating: "A cyberattack of this severity is an unlikely occurrence, but we believe that it is representative of the type of extreme events that insurers

should assess in order to understand potential exposures." Annex A to the report lists all known "cyberattacks against industrial control systems since 1999," including the 2013 attack on the San Jose power station that Ted Koppel begins with in "Lights Out."

Conclusion

While the likelihood of a massive cyberattack on the United States power grid appears to be remote for now, these two publications raise awareness of the ramifications if such a strike were to occur.

They also provide some guidance on steps we can take to minimize the risk and address our insurance needs.