AN A.S. PRATT PUBLICATION
OCTOBER 2023
VOL. 9 NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 NUMBER 8 October 2023

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2023–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Power Grids and Points of Vulnerability: Keeping the Lights on Amid Cybersecurity Concerns

By Alicia M. McKnight and Brian E. Finch*

In this article, the authors state that all energy industry players should evaluate the cybersecurity risks of our increasingly interconnected, internet-enabled power grid.

Although that new smart refrigerator might seem like a fun gadget and great way to sync up grocery lists, smart appliances have the potential to become vectors in malicious power grid attacks. Or what about the increasingly popular addition of a solar plus storage solution or an EV charging station in individual homes? These home energy hubs, connected to the power grid and often linked with a host of devices via a mobile phone, pose another layer of risk that is only beginning to be explored.

While the World Economic Forum has drawn attention[1] to a worldwide "cyber pandemic," electrical grid breaches remain an ongoing point of alarm. Power grids are more exposed than ever to cyberattacks, thanks in part to the vast expansion of (often poorly secured) consumer internet-connected devices, large remote-work networks and new smart grid technologies that connect power meters remotely to aging grid infrastructure.

As we look to the future, the rapidly evolving technologies that are necessary to enable distributed energy resources and virtual power plants, such as residential energy storage, home energy hubs and EV bidirectional charging (V2H, V2G or V2X), have the potential to dramatically redefine those risks – for the better or the worse.

ELECTRIC GRID ATTACKS

The United States, along with many other countries, is grappling with how to protect sprawling, interconnected networks of private and public energy generating resources from cyber threats. The complex system includes 200,000 miles of transmission lines, 55,000 substations and 5.5 million miles of distribution lines. Any of these essential elements could be the aim of a cyberattack, as could any number of personal smart devices or grid-connected distributed energy resources in homes across the country.

* The authors, attorneys with Pillsbury Winthrop Shaw Pittman LLP, may be contacted at alicia.mcknight@pillsburylaw.com and brian.finch@pillsburylaw.com, respectively.

[1] https://www.weforum.org/agenda/2021/10/protecting-critical-infrastructure-from-cyber-pandemic/.

Consider just a few of the high-profile electric grid attacks that have made headlines in recent years:

- During the winter of 2015, hackers working for the Russian government knocked out Ukraine's power grid,[2] switching off lights and warmth to more than 200,000 Ukrainians. Just a year later, they did it again – this time taking out about a fifth of the power consumption in Kyiv for an hour. The second attack demonstrated an alarming new level of capabilities that some experts say could be employed on any electric transmission site in the world.

- In another hit to Ukraine, in 2017 attackers used malware[3] stolen from the U.S. National Security Agency to freeze computers in hospitals, grocery stores and even radiation-monitoring systems at the old Chernobyl nuclear plant. The complex attacks inflicted collateral damage to the tune of $10 million worldwide, and at major corporations including Rosfneft, a Russian state-owned energy company.

- As recently as April 2022, using the same malware from the 2016 attack, Russian hackers came close to another massive electric grid takedown[4] in Ukraine that would have left two million people in the dark. Though they were thwarted, intelligence officials then said that in its ongoing conflict with Ukraine, Russia would be ramping up its cyber offenses[5] for the spring 2023.

- At around the same time, it was disclosed that about a dozen U.S. power and energy stations were targeted[6] in a similar such attempt, with Russian cybercriminals believed to be at the helm of the operation. The malware was blocked, but still exists and is designed to target almost any major infrastructure system.

- In 2017 another group, whose origins are unknown, penetrated computer networks at a nuclear power plant[7] in Kansas by placing malicious links on websites frequented by employees, as well as by placing malware within highly convincing résumé attachments. Attackers specifically targeted senior engineers with access to control systems. Although the FBI and

---

[2] https://www.cnn.com/2022/03/16/politics/russia-us-cyberattack-infrastructure-invs/index.html.

[3] https://www.nytimes.com/2017/06/28/technology/ransomware-nsa-hacking-tools.html.

[4] https://www.bbc.com/news/technology-61085480.

[5] https://www.politico.com/news/2023/02/25/ukraine-russian-cyberattacks-00084429.

[6] https://www.politico.com/newsletters/power-switch/2023/02/14/this-russia-linked-hack-worse-than-we-knew-00082755.

[7] https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html.

Department of Homeland Security reported that no operations systems were breached, the attack highlights the susceptibility of sensitive energy hubs to online threats.

- A widespread outage in Mumbai[8] in 2020 is also believed to be the result of malware, which was uncovered at a load dispatch center. It took two hours for authorities to restore power to essential services, and some affected areas were offline for 12 hours.

- In another attack, hackers cut power in South Africa's largest city,[9] Johannesburg, with a virus that in 2019 targeted the locale's primary electric provider, first attacking its databases and eventually turning off the electricity.

These past cyber breaches indicate that future break-ins involving the power grid are not far-fetched, especially as more and more unsecured devices connect to the grid. Although the U.S. energy grid now operates in a digital environment with components that are internet-accessible, most plants were never designed with high-tech security in mind. Additionally, hackers are becoming increasingly sophisticated with the help of AI technology.

PREPAREDNESS

While none of this is necessarily news to the executives helming the companies in charge of crucial grids and networks, that does not mean the threat has been fully addressed.

In a 2022 cybersecurity preparedness survey of more than 150 corporate executives of organizations (with a minimum annual revenue of $500 million), 40% of respondents in the energy, mining and utilities sector admitted to not currently having a dedicated in-house team with full-time responsibility for cyber incident response. Perhaps not surprisingly, while the vast majority of TMT (86%) and financial services executives (80%) were confident in their existing cybersecurity capabilities, only 34% of energy, mining and utilities respondents felt the same.

Jon Wellinghoff, former chair of the Federal Energy Reserve Commission (FERC), told The New York Times[10] that "we never anticipated that our critical infrastructure control systems would be facing advanced levels of malware." In another

[8] https://www.securityweek.com/major-power-outage-india-possibly-caused-hackers-reports/#:~:text=The%20most%20significant%20power%20outages,to%20Russia%2Dlinked%20threat%20actors.

[9] https://thehackernews.com/2019/07/cyberattack-power-outage.html.

[10] https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html.

much-reported interview with 60 Minutes, he also revealed that a FERC report "found the U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine substations."

The stakes are high when it comes to girding electricity grids against cyberattacks. To grasp the potential consequences of widespread power failure, we need only look at a few major outages:

- Pakistan suffered a nationwide blackout[11] in January 2023 that left nearly 220 million people without electricity. Though the outage was attributed to a technical failure rather than a cyberattack, the results paint a picture of how one grid malfunction can have a cascading effect in a system of interconnected energy. Locals faced crippling disruptions. Hospitals were thrown into chaos as they lost power, and some people went without water, as water pumps relied on electricity to run.

- In Texas, a 2021 surprise winter storm[12] knocked out most of the state's power for as long as three days in some areas. The power loss led to the deaths of almost 250 Texans, many to hypothermia, and others to carbon monoxide poisoning as they tried to stay warm with portable generators. Texas is unique, as it has its own power grid independent of other states (and federal regulations), meaning that it was unable to borrow power from other states when the entire system failed, raising questions around the security risks of a fully independent power grid.

- When Superstorm Sandy[13] struck in 2012, a staggering 8.1 million homes and businesses throughout the Northeast U.S. lost power after a transformer explosion at a Manhattan substation. It took weeks (and many millions of dollars) to fully restore power, with citizens scrambling to keep food fresh without refrigeration, and to find safe drinking water. The storm was a wakeup call about the need for failsafe power grids.

To state the obvious – the modern world is not well-equipped to survive without electricity. A cyberattack on the power grid could be catastrophic – for regions and also for entire nations. Losing power is also bad business, as restoring a broken grid is costly, and regions can take major economic hits when commerce is forced to a halt.

The biggest threats come in the form of political adversaries and cybercriminals hoping for ransom money. The United States and others can benefit from modernizing aging

[11] https://www.cnn.com/2023/01/22/asia/pakistan-power-outage-intl-hnk/index.html.

[12] https://www.texastribune.org/2022/01/02/texas-winter-storm-final-death-toll-246/.

[13] https://www.reuters.com/article/us-storm-sandy-powercuts/superstorm-sandy-cuts-power-to-8-1-million-homes-idUSBRE89T10G20121030.

infrastructure in order to avoid "cascading failures" seen in places like Pakistan. Multiple federal agencies are now scrambling to determine how they can impose regulations or requirements on energy companies.

HEEDING WARNINGS

Leaders are beginning to heed warnings about fortifying power grids against hackers. President Biden issued an executive order[14] to modernize and expand cybersecurity for the U.S. power grid. The Department of Energy (DOE) also launched a $45 million initiative[15] to boost cybersecurity for the electric grid, and the IoT Cybersecurity Improvement Act of 2020 established minimum security standards for federal government devices.

Most recently, FERC approved a new cybersecurity standard[16] to address supply-chain risks within the electric system, and the DOE partnered with members[17] of the EV industry to ensure cybersecurity issues are addressed. The U.S. Government Accountability Office[18] has called for even further action, asking the DOE to conduct a full assessment of cybersecurity risks to the grid followed by a coordinated response with the Department of Homeland Security, state and industry partners.

As countries continue to move toward better oversight of these cybersecurity needs, additional legislation is sure to come. A joint effort will be needed to get the energy sector's security measures up to snuff, but many across the industry are working to make it happen.

CONCLUSION

All industry players, from a startup developing a novel technology solution to enable V2G interconnection to a developer installing commercial solar that may form part of a virtual power plant, to a conventional energy company looking to redefine its position in the energy transition, to utilities and transmission companies of all sizes should evaluate the cybersecurity risks of our increasingly interconnected, internet-enabled power grid.

---

[14] https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.

[15] https://www.energy.gov/articles/doe-announces-45-million-next-generation-cyber-tools-protect-power-grid.

[16] https://www.ferc.gov/media/e-1-rd23-3-000.

[17] https://www.energy.gov/ceser/articles/doe-ceser-leadership-attends-white-house-ev-cybersecurity-forum#:~:text=The%20event%20was%20a%20strategic%20opportunity%20for%20DOE,deployed%20with%20cybersecurity%20and%20reliability%20considerations%20in%20mind.

[18] https://www.gao.gov/blog/securing-u.s.-electricity-grid-cyberattacks.

A key tool in understanding and mitigating those risks will be conducting a risk assessment – protected by attorney-client and self-review privileges – that takes into account the latest legal developments and available countermeasures. As part of that assessment, companies and their internal legal, compliance and IT teams should develop an understanding the applicable cybersecurity regulatory framework and design a cybersecurity governance framework in light of those requirements. Regular audits of those risks and governance frameworks are also recommended in light of the rapidly evolving technology and regulatory frameworks.

Finally, if a cybersecurity breach does occur, bringing together data protection, privacy, regulatory, white collar and litigation expertise in a unified crisis management team will be critical.