Cybersecurity and Distributed Energy Resources

This fact sheet addresses cybersecurity for distributed energy resources (DERs) and identifies best practices in cybersecurity governance, technical management of cyber-physical systems, and physical security.

Growing Impact of DERs

DERs include wind, solar, battery storage, and other small-scale power devices connected at the grid edge. The deployment of DERs can support resilience through increasing overall and spatial diversity of generation resources. For example, a natural disaster or terrorist attack may remove a large, centralized generation facility from service, but dispersed DERS will not necessarily be impacted. Further enabling resilience, DERs can also be used to create "islandable" generation that continues to operate during outages. Lessons learned from widespread or longer duration outages have been used to inform more resilient DER design, as is the case in New Jersey following Hurricane Sandy ("New Jersey Board of Public Utilities Microgrid Report" 2016). Facilities with islanded generation can remain powered during a disruption, which can be particularly beneficial for critical facilities. Islanding can offer significant value in places where transmission or distribution systems may experience frequent faults caused by aging equipment, long delivery distances, shortages of trained staff with technical expertise in grid operations, extreme weather, or other factors.

Cyberattacks on the Electric Grid: Recent Examples

Year	Malware used	Target	Goal	Reference
2015	Laziok	Energy companies worldwide	Information-gathering	(Paganini 2015)
2015	BlackEnergy 3	Ukrainian electric distribution company	Power outage to 225,000 customers	(Lee, Assante, and Conway 2016)
2015-2017	Dragonfly 2.0	Energy companies in the Western United States	Information-gathering, potential access to operational systems	(Bisson 2017)
2016	Crash Override	Ukrainian electric transmission substation	Power outage to one-fifth of Kiev	(Greenberg 2017)
2019	Basic hacking toolkits	An electric utility in the Western United States	Disruption of internet-based communication	(Marks 2019)

While deployment of DERs has the potential to increase grid resilience, it also introduces new challenges to grid cybersecurity. Maintaining stable grid voltage and frequency requires entire fleets of DERs to work in a coordinated fashion, and that requires a control network connected to cyber-physical grid-edge devices. Both the control network and the devices become potential points of compromise. Ensuring the cybersecurity of DERs is, therefore, a necessary element of overall grid cybersecurity, and, thus, power sector resilience.

Fortunately, the cybersecurity best practices of many different domains can be used to inform DER cybersecurity (see Figure 1). Those best practices presented below represent a solid foundation for a comprehensive DER security program.[1]

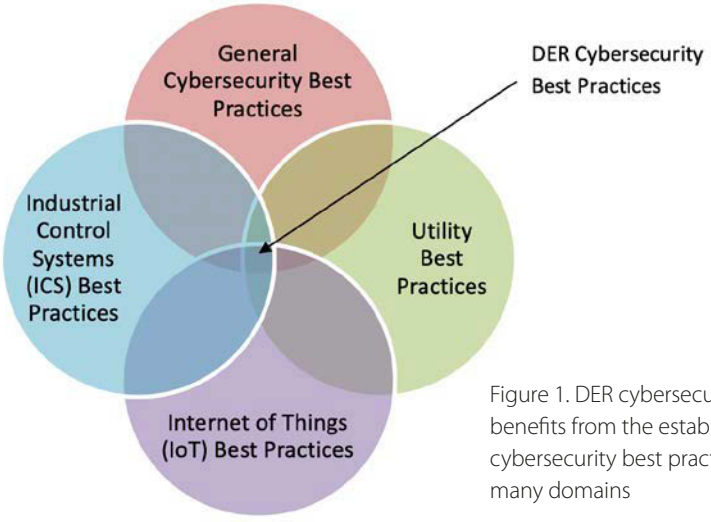

Figure 1. DER cybersecurity benefits from the established cybersecurity best practices of many domains

1 The best practices for DER cybersecurity presented here are from the National Renewable Energy Laboratory's (NREL's) Distributed Energy Resource Cybersecurity Framework (DERCF), which itself draws from many sources. The DERCF is available at https://dercf.nrel.gov.

DER Cybersecurity Governance

The cybersecurity governance pillar focuses on principles, policies, and practices. Although managers and administrators are primarily responsible for cybersecurity decisions and procedures, everyone in the organization needs to carry out these practices to protect the organization effectively. Guidance in this area is drawn from the 10 domains of the U.S. Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2); three example domains are:

Risk management: Recognizing and documenting current and potential risks to DER systems is imperative to decreasing and managing threats. An organization should develop a cybersecurity risk management plan for its overall site, focusing on preventing unauthorized access to its informational technology (IT) and operational technology (OT) platforms.

Asset management and network topology Maintaining an up-to-date catalog of IT and OT assets is an important practice for standard operations and during a potential cybersecurity attack. Furthermore, proper segmentation of the IT and OT environments prevents an attack on one system from impacting the other.

Managing supply chain risks: Monitoring an organization's external supply chain and technology vendors is also critical to protecting a DER system. Compromises to cybersecurity from outside the organization could be unintentional or malicious, and recognizing potential vulnerabilities is an important part of an organization's risk management framework.

Cybersecurity and Power Sector Resilience

Power sector resilience is "the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions to the power sector through adaptable and holistic planning and technical solutions" ("Resilient Energy Platform" n.d.). As Table 1 shows, cyberattacks are one type of threat that must be accounted for in resilience planning.

Attacks on the Ukrainian electric grid have demonstrated the ability of cyberattackers to disrupt the power sector—in one such attack, 225,000 customers lost power (Lee, Assante, and Conway 2016). Cyberattacks must, therefore, receive the same considerations as other disruptions regarding planning, response, recovery, and so on; however, unlike many other types of disruptions (for instance, a hurricane) cyberattacks are malicious in intent, and the risks posed evolve over time. Cyberattackers will change their strategy, develop new tools, and choose when they strike—possibly at a time when the system is already vulnerable due to another disruption. Malicious intent and adaptability must be accounted for in risk analysis and mitigation planning.

Table 1: Categories of Power System Threats

Natural	Technological	Human-Caused
Weather	System failures	Cyberattacks
Earthquakes	Component Failures	Accidents
Wildfires	Aging infrastructure	Physical Attack
Solar Events		
Animal Disruptions		

DER Cyber-Physical Technical Management

The cyber-physical technical management pillar is concerned with limiting electronic access to an organization's systems and devices. Restricting unnecessary entry is an important cybersecurity practice; areas of concern include:

Access control: For both local and remote system and device use, the principles of access control include least privilege (where users can access system resources only to accomplish their assigned tasks), role-based asset control (where user access to system resources is defined by job duties), and two-factor authorization (where users must supply a second form of identification to access the system).

Third-party interactions: An organization's interaction with cloud data storage and web-based technologies must be closely monitored. Organizations should be aware of the contents of agreements and documentation with third-party vendors and retain positive relationships with these providers in case of disruptions to the system from cyberattacks.

Logging and alerts: Logging of system and application events can help identify cyberattacks as they happen and aid in performing forensic analysis after an attack. A useful solution is to structure logs that trigger alerts when certain behaviors occur. These alerts can be designed to activate based on the use of a device, a specific threshold of use, or an extreme action.

DER Physical Security

The physical security pillar focuses on the importance of security controls that defend the physical infrastructure of DER organizations. Physical security is an organization's first line of defense and should include the following three components:

Holistic security and contingency planning: An organization should have a strong, layered security plan that covers monitoring of the physical security system, response, and recovery procedures, and the roles and responsibilities of key personnel. The plan should also include countermeasures to increase cybersecurity if physical security measures fail.

Intrusion detection and prevention: A second foundational layer comprises specific security controls to prevent intruders or unauthorized personnel from gaining access to the system. This includes security for the property's boundaries (e.g., fencing, gates, and barricades) and entry into buildings and other access points. Organizations should have monitoring capabilities (e.g., motion detectors, security cameras, and guard patrols) that can verify threats quickly and help improve response times.

Site-supportive equipment: Backup equipment, such as generators and high-quality cabling, should be located on-site to allow DER systems to keep running continuously in the event of an intrusion or other disruption.

Securing DERs is one part of grid cybersecurity. To effectively secure the grid, system operators must implement organization-wide cybersecurity programs that address both enterprise security and security for industrial control systems. The latter includes security for centralized generation and the communication networks that support control of remote devices, as well as timely software updates and applications that monitor the system for cyber intrusion. While this fact sheet covers DERs specifically, planning for cybersecurity across the entire power system is crucial. The "More Resources" section below provides publications that support broader cybersecurity planning efforts.

Resilient Energy Platform

The Resilient Energy Platform helps countries and localities address power system vulnerabilities by providing strategic resources and directing country support to enable planning and deployment of resilient energy solutions. This includes curated reference material, training materials, data, tools, and direct technical assistance in planning resilient, sustainable, and secure power systems. Ultimately, these resources enable decision makers to assess power sector vulnerabilities, identify resilience solutions, and make informed decisions to enhance energy sector resilience at a range of scales, including local, regional, and national. To learn more about the technical solutions highlighted in this fact sheet, visit the Resilient Energy Platform website at: https://resilient-energy.org/.

References

Bisson, David. 2017. "Dragonfly 2.0 Attack Campaign Targets Western Energy Sector." *The State of Security* (blog). September 6, 2017. https://www.tripwire.com/state-of-security/latest-security-news/dragonfly-2-0-attack-campaign-targets-western-energy-sector/.

Greenberg, Andy. 2017. "Crash Override Malware Took Down Ukraine's Power Grid Last December." *Wired*, June 12, 2017. https://www.wired.com/story/crash-override-malware/.

Marks, Joseph. 2019. "The Cybersecurity 202: A Cyberattack Just Disrupted Grid Operations in the U.S. But It Could Have Been Far Worse." *Washington Post*, May 6, 2019. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/05/06/the-cybersecurity-202-a-cyberattack-just-disrupted-grid-operations-in-the-u-s-but-it-could-have-been-far-worse/5ccf61eda7a0a46cfe152c3e/.

"New Jersey Board of Public Utilities Microgrid Report." 2016. New Jersey Board of Public Utilities. https://www.nj.gov/bpu/pdf/reports/20161130_microgrid_report.pdf.

Paganini, Pierluigui. 2015. "Energy Companies Infected by Newly Laziok Trojan Malware." *Security Affairs* (blog). April 1, 2015. https://securityaffairs.co/wordpress/35567/cyber-crime/energy-companies-laziok-trojan.html.

"Resilient Energy Platform." n.d. Resilient Energy Platform. Accessed February 7, 2020. https://resilient-energy.org.

Photo from iStock 1182411756

Lee, Robert M., Michael J. Assante, and Tim Conway. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid." E-ISAC & SANS ICS. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

U.S. Department of Energy. *Electric Sector Cybersecurity Capability Maturity Model* (ES-C2M2). Version 1.1. Washington, D.C., 2014. https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

More Resources

Carter, Cedric, Ifeoma Onunkwo, Patricia Cordeiro, and Jay Johnson. 2017. "Cyber Security Assessment of Distributed Energy Resources." https://www.researchgate.net/publication/319206165_Cyber_Security_Assessment_of_Distributed_Energy_Resources.

Cleveland, Frances, and Annabelle Lee. 2013. *Cyber Security for DER Systems*. NESCOR Grant DE-OE0000524. Palo Alto, CA: Electric Power Research Institute. http://smartgrid.epri.com/doc/der%20rpt%2007-30-13.pdf.

Cook, Jeffrey J, Christina Volpi, Erin Nobler, and Kyle Flanegin. 2018. "Check the Stack: An Enabling Framework for Resilient Microgrids." Technical Report NREL/TP-6A20-71594. National Renewable Energy Laboratory. https://www.nrel.gov/docs/fy19osti/71594.pdf.

Cornell, Phillip. 2020. "International Grid Integration: Efficiencies, Vulnerabilities, and Strategic Implications in Asia." *Atlantic Council* (blog). January 9, 2020. https://www.atlanticcouncil.org/in-depth-research-reports/report/international-grid-integration-efficiencies-vulnerabilities-and-strategic-implications-in-asia/.

EECSP (Energy Expert Cyber Security Platform). 2017. *Energy Expert Cyber Security Platform: Cyber Security in the Energy Sector*. European Commission. https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf.

Keogh, Miles, and Sharon Thomas. 2017. *Cybersecurity: A Primer for State Utility Regulators*. Washington, D.C.: National Association of Regulatory Utility Commissioners. https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.

Lai, Christine, Nicholas Jacobs, Shamina Hossain-McKenziezie, Cendric Carter, Patricia Cordeiro, Ifeoma Onunkwo, and Jay Johnson. 2017. *Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators*. SAND2017-13113. Albuquerque, NM: Sandia National Laboratories. https://www.researchgate.net/publication/322568288_Cyber_Security_Primer_for_DER_Vendors_Aggregators_and_Grid_Operators.

NARUC (National Association of Regulatory Utility Commissioners). "Cyber Evaluative Framework for Black Sea Regulators." 2017.

NIST (National Institute of Standards and Technology). 2018. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1." https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

NIST. 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*. Special Publication 800–53. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Powell, Charisa, Konrad Hauck, Anuj Sanghvi, and Tami Reynolds. 2020. *Distributed Energy Resource Cybersecurity Framework Best Practices*. NREL/TP-5R00-75921. Golden, CO: National Renewable Energy Laboratory. https://www.nrel.gov/docs/fy20osti/75921.pdf.

Qi, Junjian, Adam Hahn, Xiaonan Lu, Jianhui Wang, and Chen-Ching Liu. 2016. "Cybersecurity for Distributed Energy Resources and Smart Inverters." *IET Cyber-Physical Systems: Theory & Applications* 1 (1): 28–39. https://doi.org/10.1049/iet-cps.2016.0018.

Silverstein, Ken. 2019. "Distributed Energy Resources to Grow 15.9% CAGR." *Microgrid Knowledge*. June 24, 2019. https://microgridknowledge.com/distributed-energy-resources-navigant/.

Stamber, Kevin, Andjelka Kelic, Robert Taylor, Jordan Henry, and Jason Stamp. 2017. *Distributed Energy Systems: Security Implications of the Grid of the Future*. SAND2017-0794. Albuquerque, NM: Sandia National Laboratories. http://prod.sandia.gov/techlib/access-control.cgi/2017/170794.pdf.

Sundararajan, Aditya, Aniket Chavan, Danish Saleem, and Arif I. Sarwat. 2018. "A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security." *Energies* 11 (9): 2360. https://doi.org/10.3390/en11092360.

Photo from iStock 1140211998

Wang, Jianhui. 2016. "Cybersecurity for Renewables, Distributed Energy Resources, and Smart Inverters." Presented at the Cybersecurity for Energy Delivery Systems Peer Reviewe, Argonne National Laboratory, December 7, 2016. Lemont, IL. https://www.energy.gov/sites/prod/files/2017/02/f34/ANL_Peer_Review_2016_cybersecurity_for_renewables.pdf.

Westerhof, Willem. n.d. "Horus Scenario." Horus Scenario. https://horusscenario.com/.

www.resilient-energy.org | www.nrel.gov/usaid-partnership

Jeremy Foster
U.S. Agency for International Development
Email: jfoster@usaid.gov

Sarah Lawson
U.S. Agency for International Development
Email: slawson@usaid.gov

Sadie Cox
National Renewable Energy Laboratory
Email: sadie.cox@nrel.gov

This work was authored, in part, by the National Renewable Energy Laboratory (NREL), operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the United States Agency for International Development (USAID) under Contract No. IAG-17-2050. The views expressed in this report do not necessarily represent the views of the DOE or the U.S. Government, or any agency thereof, including USAID.

NREL/FS-5R00-76307 | April 2020
NREL prints on paper that contains recycled content.

The Resilient Energy Platform provides expertly curated resources, training, tools, and technical assistance to enhance power sector resilience. The Resilient Energy Platform is supported by the U.S. Agency for International Development.

The USAID-NREL Partnership addresses critical challenges to scaling up advanced energy systems through global tools and technical assistance, including the Renewable Energy Data Explorer, Greening the Grid, the International Jobs and Economic Development Impacts tool, and the Resilient Energy Platform. More information can be found at: **www.nrel.gov/usaid-partnership**.

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

REexplorer MAPPING OUR ENERGY FUTURE

Greening the Grid

I-JEDI

Resilient Energy Platform