Deloitte.

5x5 series: Insights and actions

Securing distributed energy resources

Distributed energy resources (DERs) are driving innovation across the electric grid. Along with this shift, DERs pose new cybersecurity considerations that require non-traditional solutions. Securely deploying DERs could help mitigate cybersecurity risks; prepare for future regulation; enable DER expansion; and allow utilities to continue to provide safe, reliable, resilient, and secure energy to their customers.

5 things you should know

Growing digital interconnections between DERs, associated third parties, and utilities could expand the cybersecurity threat surface.

Unlike traditional Operational Technology (OT) devices, **DERs are increasingly internet-facing and utilize cloud-based solutions for aggregating and analyzing data** used to make operational decisions. This may expand the attack surface and introduce additional risk through added complexity to the environment that would need to be addressed.

Federal and industry entities are publishing cybersecurity guidelines that are driving states to **adopt DER cybersecurity standards.**

DERs introduce many third parties into grid operations which creates **new supply chain risks** that may not be able to be addressed through existing controls and programs.

DER aggregators, DER owners/operators, and related third parties, such as system integration and engineering services, should **collaborate to address cybersecurity concerns.**

5 actions you can take

1 Adopt standards for DER interconnections to **drive consistency in DER management.** Develop data models including controls to secure the availability, integrity, and confidentiality of data. Leverage automated tools to maintain interconnection inventories and to monitor interconnections. Develop responsibility matrices to clearly define security responsibilities for DER system integrators, DER owners/operators, DER aggregators, and utilities.

2 Develop standard architecture templates and standard **security controls to address internet-facing capabilities** and use of cloud in DER management. Enforce cyber-informed engineering when integrating DERs to decrease inherent cyber risks and vulnerabilities which could require additional costs to mitigate after deployment. Engage with cloud providers, original equipment manufacturers (OEMs), and DER owners/operators to set expectations on securing internet and cloud usage. Establish and automate testing of DER software.

3 Be proactive with DER security instead of reacting to future regulation. Participate in the decision-making process when solicited for feedback. Stay educated on recent and upcoming regulations and standards. **Build DER security practices** into standard build and interconnection methodologies.

4 Define roles and responsibilities between entities in the supply chain. **Add cybersecurity language to interconnection agreements**. Develop standards depending on the type of entity engaged with as part of a DER project or interconnection. Add steps to conduct due diligence to mitigate risks related to data sharing with foreign adversaries, components-sourcing linked to forced labor, and foreign control of third parties.

5 Adopt cyber-informed engineering practices when developing new DERs and during interconnection projects. **Include cybersecurity as a specific component to DER strategies**. Develop business cases and gain executive alignment on investing in cybersecurity for DERs.

Connect with us:

David Novak
Principal
Deloitte & Touche LLP
danowak@deloitte.com

Sam Icasiano
Managing Director
Deloitte & Touche LLP
saicasiano@deloitte.com

Allison White
Senior Manager
Deloitte & Touche LLP
alliwhite@deloitte.com