Deloitte.

5x5 series: Insights and actions

Securing renewable power generation

The proliferation of renewable power generation sites is transforming them into integral components of grid operations. Given the number of stakeholders involved, protecting these sites from cyberattacks may appear a bit challenging. Original equipment manufacturers (OEMs), operations, maintenance, regulators, and joint venture ownership can complicate the implementation of good cybersecurity practices. Despite these complexities, it is critical to prioritize the establishment of robust cybersecurity protocols. By taking steps to analyze vulnerabilities, quantify risk, and develop good cybersecurity governance policies, a site-specific mitigation roadmap might help decrease exposure to cyber incidents.

***5** insights you should know*		***5** actions you can take*
Cyberattacks on critical power infrastructure are on the rise from many different threat actors. Understanding where gaps and vulnerabilities exist in control systems and the physical security of those systems is imperative to reduce cybersecurity attack surfaces.	1	Conduct an Industrial Control Systems (ICS) **cybersecurity framework assessment** using National Institute of Standards and Technology (NIST) guidelines and International Society of Automation (ISA) 62443 standards, developed specifically for control systems to identify gaps, risks, and vulnerabilities throughout the implementation and operation of sites. This may help you focus on prioritizing remediation activities to reduce risk.
Vulnerabilities themselves are not risks. It is important to identify and quantify actual risks associated with specific gaps and vulnerabilities to allocate resources to mission-critical systems. Risk systems used in information technology (IT) systems may not translate well into operational technology (OT) systems—therefore, it is important to assess vulnerabilities and risks using tools specifically for OT systems.	2	Conduct a **cyber risk and attack surface management assessment** to assess and quantify risks and vulnerabilities specific to OT systems. Leveraging familiar terminology and methods used in safety operations, results of these assessments produce easy-to-understand quantification of risks associated with cyber, safety, environmental, financial, regulatory, and reputational impacts.
Plant operations personnel, including third-party contractors accessing OT sites, are not often trained on how to identify and respond to cybersecurity events. **Onsite cybersecurity training should be standard at each site**—the same way safety training is required.	3	**Develop site-specific general and role-based cybersecurity training sessions,** and expect site visitors to participate when visiting sites. Instruct plant operations personnel to complete mandatory cybersecurity training, including regular exercising of incident response procedures to build muscle memory in responding to cyber events.
The scale and criticality of industrial systems make **the identification of vulnerabilities and crown jewel assets a major industrial challenge.** Mitigation efforts are confined within the planned maintenance windows, and security teams should focus their efforts on relevant assets.	4	**Perform a vulnerability rationalization analysis combined with a business impact analysis** to help the security team identify mission-critical assets and provide insights on active attack paths that could lead to a major business impact. This analysis should be periodically repeated to provide regular insights to help the security team manage active attack surfaces.
Cyber risk isn't just about the local controls. It extends into the Cloud, across third-party networks through edge devices and to connected devices. High connectivity creates a dynamic tech stack, and organizations should enrich their capabilities through new technologies.	5	**Develop and implement cybersecurity governance policies for OT systems** and incorporate into third-party service and supply agreements. This is an important factor in maintaining good cyber hygiene and program maturity in the OT environment.

Want to see this live?
Visit us at the Cyber IoT Studio or *The Smart Factory at Wichita State University!*

Connect with us:

Wendy Frank
Principal
Cyber OT Leader
Deloitte & Touche LLP
wfrank@deloitte.com

Ramsey Hajj
Principal
Cyber IOT
Deloitte & Touche LLP
rhajj@deloitte.com

Anne Robbins
Senior Manager
Cyber IoT
Deloitte & Touche LLP
anrobbins@deloitte.com

Rishabh (George) Das, PhD
Specialist Master
Cyber IoT
Deloitte & Touche LLP
rishadas@deloitte.com

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

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2024 Deloitte Development LLC. All rights reserved.