Deloitte.

Critical infrastructure 5x5: Insights and actions

Bulk electric system (BES) resiliency

Attacks on critical infrastructure are increasing, as evidenced by a recently growing number of physical security attacks on the bulk electric system, impacting both reliable operations and customer service. Cyber security and physical security are converging to present critical infrastructure providers with the challenge to effectively prevent, detect, and respond to these types of attacks.

How can your organization be better prepared to avoid and/or mitigate damages from an attack? Read more here.

***5** things you should know*		***5** actions you can take*
Public safety is at risk. Attackers are expanding their methods of attack, including a more recent focus on physical attacks on vulnerable essential facilities and equipment as a mechanism to achieve their objective.	1	Be as prepared for the unexpected as you can be. Accelerate the use of this scenario to **conduct crisis and resiliency drills**, tabletops, and red teams for business-critical regulated facilities and assets. ***Learn more*** about how Deloitte can help you respond swiftly and effectively to high-impact events.
Physical attacks and cyberattacks are merging. Bad actors are planning coordinated attacks, leveraging weak points in physical and cybersecurity controls to affect their critical infrastructure targets. Advancements in physical security controls are increasingly leveraging cyber technology, and cyber assets remain vulnerable to simple physical attacks.	2	Gates are not enough. **Review and update physical security** cameras, monitoring, and protections, and make special considerations for robotic surveillance and other technology-enabled physical security programs. Deloitte can help you ***build resilient digital operations*** and ***protect your enterprise*** with secure, connected devices.
Additional **regulatory action is likely on the way**. As has happened in the past after high-profile critical infrastructure attacks, there will likely be a wave of new and/or updated regulations aimed at mitigating these types of attacks in the future.	3	Refresh your critical infrastructure controls and protections to **consider public safety impact in addition to reliability**. Model and consider ***dynamic risk programs*** to proactively and more effectively manage risk, compliance, and crisis scenarios to increase confidence.
Your closest allies could be increasing your risk. As attackers are getting more creative, they are increasingly leveraging trusted suppliers in your supply chain as an attack vector to achieve their objective. Many supply chain risk programs focus on contractual obligations for new vendor relationships, missing the risk from the population of existing suppliers and practical controls to mitigate supply chain risk.	4	**Update your supply chain risk management program** to help protect your critical infrastructure from a supply chain attack. Consider continuous security risk monitoring programs for your highest-risk third-party relationships, along with Zero Trust Access control to protect your environment. Leverage the latest innovations and techniques to provide a ***secure supply chain.***
You need to be in the know. After recent attacks, open-source intelligence and social media were filled with competing theories, misinformation, false-flag claims—and very few attributable details.	5	**Expand your threat intelligence program.** Get in front of a potential event. Converge your information technology, operational technology, and physical security threat detection and preparedness. Experience the difference an ***enhanced security posture*** can make in the face of threats and disruptions.

Let's talk about how you can further secure your critical infrastructure.

Connect with us:

SHARON CHAND
Principal | Cyber Risk Services
shchand@deloitte.com

BRAD SINGLETARY
Managing Director | Cyber Risk Services
bsingletary@deloitte.com