Tips

Cybersecurity Threats to Critical Infrastructure

Critical infrastructure systems face potential cyberattacks across all organizations. Are you prepared? The 10 points below cover the most critical hazards and immediate protective actions (items 1–7 are hazards & items 8–10 are protective actions).

1. **Chemical Dosing Manipulation:** Unauthorized changes to water treatment controls can cause contamination or the release of toxic chemicals.
2. **Power System Disruption:** Cyberattacks on power infrastructure affect hospitals, emergency services, HVAC, and traffic signals.
3. **9-1-1 and Dispatch are Disabled:** Compromised communications systems delay or prevent emergency response when it matters most.
4. **Public Warning Systems Jammed:** Populations are left without life-safety notifications during active emergencies.
5. **Falsified Sensor Data:** Control room operators lose accurate situational awareness, leading to dangerous real-time decisions.
6. **Cascading System Failures:** One compromised node can trigger failures across interconnected infrastructure systems.
7. **Workers Exposed to Hidden Hazards:** When safety alert systems are disabled, employees encounter dangerous conditions without warning.
8. **Separate OT/ICS from IT Networks:** Use air gaps or strict firewall rules to isolate industrial control systems from corporate networks.
9. **Require Multi-factor Authentification:** Enforce MFA on all remote and administrative access points to secure systems.
10. **Train Every Employee, Not Just IT:** All staff must be able to recognize phishing, social engineering, and physical security threats.

CIRSA

Call 1.800.228.7136 | CIRSA.org