CIRSA HAZARD ALERT

Published by the CIRSA Risk Control Department | SAFER TOGETHER

Hazard Alert: Cybersecurity Threats to Critical Infrastructure

Cyberattacks targeting critical infrastructure are increasing across all sectors. Organizations of all sizes in government, utilities, healthcare, education, transportation, and private industry are potentially at risk. This hazard alert identifies key safety hazards and protective measures to help assess potential threats.

POTENTIAL SAFETY HAZARDS

A successful cyberattack can move beyond data loss into direct physical damage. The following categories represent the primary safety hazards associated with infrastructure hacking.

WATER & UTILITY SYSTEMS

- Manipulation of chemical dosing controls in water treatment, risking contamination or toxic release.
- Disruption of power systems affecting hospitals, emergency services, traffic signals, and HVAC.
- Unauthorized commands to industrial equipment causing potential fires, explosions, or hazardous spills.

EMERGENCY & PUBLIC SAFETY

- Disabling 911 dispatch or first responder communications systems.
- Interference with public warning systems, leaving populations without emergency notifications.

3665 Cherry Creek North Drive • Denver Colorado 80209 • 303-757-5475 • 800-228-7136 • CIRSA.org

Cybersecurity Threats to Critical Infrastructure (cont.)

- Traffic signal or transit system manipulation creating potential collision and evacuation risks.

CONTROL SYSTEMS & SITUATIONAL AWARENESS

- Loss of visibility in control rooms due to falsified sensor data or locked-out dashboards.
- Cascading failures across interconnected systems, where a single compromised node can affect many others.
- Corrupted safety-critical data affecting operator decisions in real time.

WORKFORCE & RESPONSE

- Disabled safety alert systems can leave workers exposed to hazards without timely warning.
- Cyber-related disruptions may lead first responders to operate on bad, incomplete, inaccurate, or manipulated intelligence during emergencies.
- Vulnerable populations, including those receiving care at hospitals and other care facilities, may lose access to life-sustaining services.

PREVENTATIVE MEASURES & BEST PRACTICES

The following categories suggest preventative measures and best practices for assessing and preventing cybersecurity attacks.

1. **NETWORK SEGMENTATION & ACCESS CONTROL**

- Isolate OT (operational technology) and ICS (industrial control systems) from corporate IT networks using air gaps or strict firewall rules.
- Implement zero-trust architecture, and verify every user, device, and connection.
- Apply least-privilege access so personnel can access only those systems they need to perform their authorized functions.
- Use multi-factor authentication (MFA) across all remote and administrative access points.

2. **ASSET VISIBILITY & PATCH MANAGEMENT**

- Maintain a complete, current inventory of all hardware and software assets.
- Prioritize patching for internet-facing systems and known exploited vulnerabilities.
- Where patching legacy OT systems is not possible, layer compensating controls such as monitoring and network isolation.

3. **ASSET VISIBILITY & PATCH MANAGEMENT**

- Deploy continuous monitoring via a Security Operations Center (SOC) or managed detection and response (MDR).
- Use IDS/IPS tuned for OT protocols (Modbus, DNP3, BACnet).
- Establish baseline 'normal' behavior so anomalies trigger alerts quickly.

Cybersecurity Threats to Critical Infrastructure (cont.)

4. **INCIDENT RESPONSE & RESILIENCE**

- Develop and regularly test an Incident Response Plan specific to OT/ICS environments.
- Conduct tabletop exercises simulating ransomware, supply chain attacks, and nation-state intrusions.
- Maintain offline, tested backups of critical system configurations and data.
- Ensure manual/analog fallback procedures exist for essential services.

5. **SUPPLY CHAIN SECURITY**

- Vet third-party vendors and contractors with access to critical systems.
- Review software bills of materials (SBOM) for dependencies.
- Limit and monitor all remote access from vendors.

6. **PERSONNEL & CULTURE**

- Train all staff, not just IT, in phishing, social engineering, and physical security.
- Conduct insider threat awareness programs.
- Enforce clean desk and physical access policies at control facilities.

7. **REGULATORY & FRAMEWORK ALIGNMENT**

- Use NIST CSF 2.0 and ICS-CERT guidance as baseline frameworks
- For water, energy, and transportation sectors, align with sector-specific requirements: NERC CIP for electric utilities, AWIA for water systems, etc.
- Engage with free assessments and resources for municipal and regional operators made available by the Cybersecurity Advisory Program (CISA).

The information and suggestions in this Hazard Alert should not be regarded as exhaustive and may not be universally applicable to every organization or system environment. Accordingly, organizations should consult with qualified IT professionals, cybersecurity personnel, legal counsel, and other appropriate consultants when assessing cybersecurity risks, evaluating potential threats, and implementing protective measures tailored to their specific operations and infrastructure.

The CISA (Cybersecurity Advisory Program) offers free vulnerability assessments and technical assistance for municipal and regional operators. This is a valuable no-cost resource for the communities you serve. CIRSA also offers members access to KnowBe4, the largest integrated platform for cybersecurity awareness training. Cyberattacks on critical infrastructure are no longer a distant threat; they are an active and growing potential risk for municipalities of every size. As this Hazard Alert has outlined, a successful attack can move well beyond data loss, triggering physical consequences that endanger workers, disrupt emergency services, and compromise public safety.

(Available resources listed on next page.)

Cybersecurity Threats to Critical Infrastructure (cont.)

RESOURCES

FEDERAL AGENCIES & FRAMEWORKS

CISA — Cybersecurity & Infrastructure Security Agency

Free vulnerability assessments, training, and 24/7 incident response support for all sectors.

- www.cisa.gov

NIST — NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

NIST Cybersecurity Framework (CSF) and SP 800-53 security controls catalog — the industry gold standard for risk assessment.

- www.nist.gov/cyberframework | csrc.nist.gov/publications

FBI CYBER DIVISION

Report cyberattacks, ransomware incidents, and infrastructure threats. Coordinates with CISA on major incidents.

- www.fbi.gov/investigate/cyber | IC3.gov (Internet Crime Complaint Center)

TRAINING & AWARENESS

CISA Free Cybersecurity Training

Role-based training for IT staff, executives, and general employees. Includes phishing awareness and ICS/SCADA security courses.

- www.cisa.gov/cybersecurity-training-exercises

SANS INSTITUTE — CYBER ACES (FREE)

Free foundational cybersecurity courses covering networking, operating systems, and security fundamentals.

- www.sans.org/cyberaces

INCIDENT RESPONSE & REPORTING

Report a Cyber Incident to CISA

- https://www.cisa.gov/reporting-cyber-incident | 1-888-282-0870

MS-ISAC — Multi-State Information Sharing & Analysis Center

Free cybersecurity services for state, local, tribal, and territorial government entities. Includes 24/7 SOC support.

- www.cisecurity.org/ms-isac