DAMS SECTOR CYBERSECURITY

Sector Overview

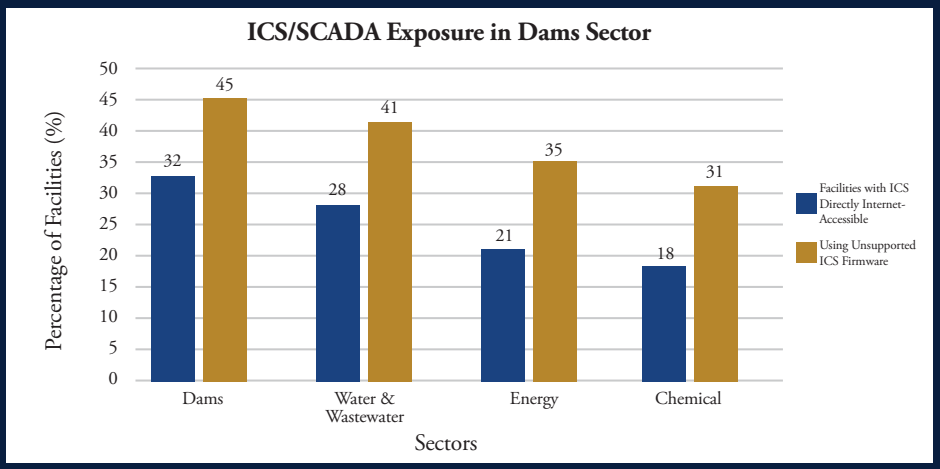
This resource is for stakeholders in Florida's Dams sector. It includes:

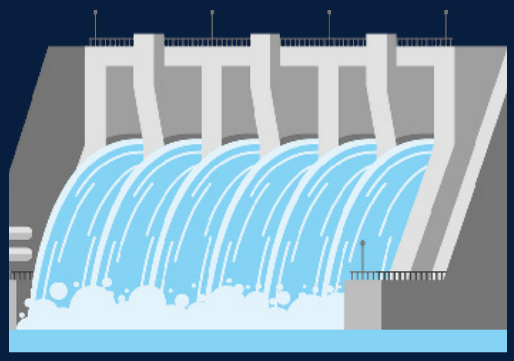
- Dam owners
- Flood control authorities
- Hydroelectric power facilities
- Operators
- Related emergency management agencies
- Water control districts

Florida's dams are smaller and fewer than in many other states, yet they are essential for water supply, flood risk reduction, navigation, recreation, and some power generation. Ransomware attacks could disrupt flood control operations and threaten downstream communities. They may also cut off water supply and hinder energy production.

Ransomware Threat Profile

Although the Dams sector is targeted less often than Energy or Water & Wastewater, its role in public safety and infrastructure still makes it a target for both criminal and nation-state actors. Many facilities rely on industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) technology that were not designed with modern cybersecurity features.





Note: The Dams sector has the highest proportion of facilities with internet-accessible ICS (32%) and unsupported ICS firmware (45%) among ICS-heavy sectors. Both exceed Water & Wastewater sector levels of 28% and 41%.

Top Vulnerabilities

- **Gate and Spillway Control System Weaknesses**
  - Floodgates, spillways, and turbine controls often use legacy ICS/SCADA platforms without modern authentication or encryption. This makes them vulnerable to ransomware that can lock operators out of water control systems.
- **Upstream–Downstream Network Exposure**
  - Administrative IT networks are often connected to dam control systems. A ransomware infection in business systems can spread to operational controls, disrupting water releases or triggering emergency spillway activation.
- **Underfunded Cybersecurity Operations**
  - Many municipal and special district operators have limited budgets and no full-time cybersecurity staff, limiting monitoring and response capabilities.
- **Third-Party Maintenance Access Risks**
  - Vendors servicing turbines, gate actuators, and monitoring sensors often have remote access for diagnostics. Without MFA and active monitoring, these connections can be exploited by attackers.
- **Weather-Event Vulnerability Windows**
  - Attackers may strike during heavy rain or hurricanes, when dam systems are under stress and recovery delays could cause flooding, property damage, or safety hazards.

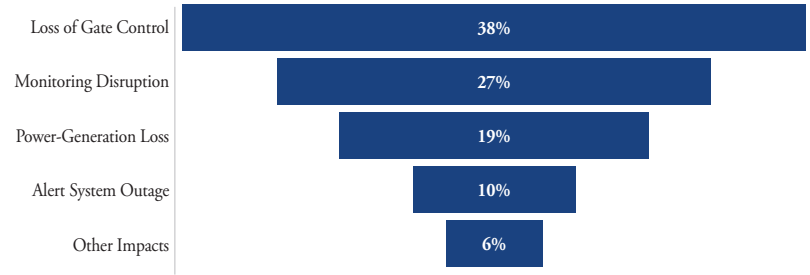
FIU Jack D. Gordon Institute for Public Policy
JGI@fiu.edu
CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA

DAMS SECTOR CYBERSECURITY

Action Checklist

- Develop and update ransomware-specific Incident Response Plans for dam gate, spillway, and turbine controls, including coordination with local emergency managers.
- Enforce Multi-Factor Authentication (MFA) for all remote and vendor ICS/SCADA access controlling water flow and flood mitigation.
- Conduct annual ransomware-specific tabletop exercises simulating operational lockouts during heavy rainfall, hurricanes, or emergency water releases.
- Implement strict network segmentation between business IT and dam operational systems to prevent ransomware crossover.
- Upgrade or securely isolate legacy ICS hardware/software for floodgates, pumps, and power generation from internet-facing networks.
- Maintain secure offline backups of operational data, configuration files, and control logic to enable rapid restoration of gate and spillway functions.
- Assign a dedicated cybersecurity lead (CISO or equivalent) or designate trained personnel to oversee OT security.

Operational Impacts of Cyber Incidents in Dams Sector



Note: Loss of gate control (38%) and monitoring disruption (27%) are the most common operational impacts. These are followed by power generation loss (19%), alert system outages (10%), and other impacts (6%).

Notable Incidents

- **American Water Cyberattack (2024):** The nation's largest water utility suspended billing systems after detecting a cyberattack. Operations continued, but the breach exposed weaknesses in business network security.
- **Lake Okeechobee Control System Disruption – Simulated Exercise (2023):** A statewide cybersecurity exercise simulated ransomware locking operators out of Herbert Hoover Dike floodgate controls. The scenario showed how delayed water releases could threaten farms, downstream towns & municipal water systems.
- **St. Johns River Water Management District Cyber Incident (2023):** Suspicious IT activity consistent with a ransomware attempt targeted the agency overseeing regional water supply governance. The threat was contained before operations were affected.
- **Central Florida Hydroelectric Facility Breach (2022):** Ransomware affected administrative and monitoring systems at a small hydroelectric plant. While power generation continued, the attack disrupted reporting to water authorities & required costly recovery.

ACTION

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **U.S. Army Corps of Engineers Dams Sector Security & Resilience Program**
- **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)**

Templates & Planning

- **Cyber Florida Incident Response Plan Templates**
  Available Upon Request
- **NIST Cybersecurity Framework**
  (https://www.nist.gov/cyberframework)
- **Dams Sector Crisis Management Handbook (DHS)**

State-Funded Resources

- **FIU Cyber Leadership Courses**
  (https://gordoninstitute.fiu.edu/cybersecurity-policy/training/cybersecureflorida/index.html)
- **CISA Cyber Hygiene Services**
  Free Assessments & Scans
  (https://www.cisa.gov/resourcestools/ programs/cyberhygiene-services)

FIU Jack D. Gordon Institute for Public Policy
JGI@fiu.edu
CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA