www.hometownconnections.com
12081 W. Alameda Parkway, # 464
Lakewood, CO 80228
P — 970 682 4217

Hometown Connections

# Top 10 Cybersecurity Considerations For Community-Owned Utilities

Utilities in the United States are prime targets for cyber attack. Criminals are hijacking utility information systems and demanding ransom for their release. Nation states and other bad actors are rehearsing ways to interrupt utility services and throw the nation into chaos. Community-owned utilities of all sizes and structures must shore up their cyber defenses. Here are the top 10 cybersecurity considerations for community utilities and their city departments:

1. **Does your cybersecurity program cover all utility services (e.g., electric, water, wastewater, gas) and city departments?**

   Among utility and other city departments, data may exist in disconnected silos that produce business inefficiencies. Whether connected or separate, none of this data is immune from cyber attack. Every city employee, utility employee, and governing official plays a key role in maintaining a cyber defense that protects business data and operations. Everyone must follow policies and procedures that prevent clicking on suspicious emails, downloading infected files, and accessing unsecured home WiFI networks for teleworkers. There must be strict rules and required training about information system access for new, continuing, and departing employees.

2. **Are you evaluating technology, policies, and controls according to industry guidelines and state/federal rules for privacy and cybersecurity?**

   Each community-owned utility must determine which cybersecurity and privacy regulations apply and which industry guidelines to follow.

   - The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a set of requirements designed to secure the assets required for operating North America's bulk electric system. These regulations are mandated and enforced by the Federal Energy Regulatory Commission (FERC). All owners and operators of the **bulk power system** must meet the mandatory nine NERC CIP standards to avoid heavy fines for non-compliance. [A bulk power

system (BPS) is a large interconnected electrical system made up of generation and transmission facilities and their control systems. A BPS does not include facilities used in the local distribution of electric energy.] Therefore, the NERC CIP requirements do not apply to every community-owned utility. However, whether or not your utility or city is required to comply with federal cybersecurity standards, NERC CIP is a strong starting point for creating your cybersecurity program.

- If the federal cybersecurity regulations do not apply to your utility or city, the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity provides a solid starting point for building your cybersecurity program. It provides controls to enhance the cybersecurity framework, risk posture, information protection, and security standards of all organizations.

- The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) was enacted to set standards for protecting consumer information. On November 1, 2007, the FACT Act was amended to include Red Flag guidelines or the Red Flags Rule, for the detection, prevention, and mitigation of identity theft. The Red Flags Rule is enforced by the Federal Trade Commission (FTC) and applies to "financial institutions" and 'creditors" with "covered accounts." Utility companies are considered creditors since service is extended prior to payment and, therefore, have two categories of "covered accounts":
    - Personal, family, or household purposes involving or designed to permit multiple payments or transactions.
    - Accounts that carry a reasonably foreseeable risk of identity theft.

  The Red Flags Rule specifies how businesses and organizations with "covered accounts" must develop, implement, and administer a written Identity Theft Prevention program. More information on this rule can be found at (Federal Register, Vol. 72. Pgs. 63718-74 (Nov. 9, 2007), 16 CFR, Part 681) or ecfr.gov.

**3. Does your plan cover OT (e.g., metering, SCADA, GIS, outage management) and IT security?**

For utilities, operations technology (metering, SCADA, GIS, outage management, etc.) can have different cybersecurity requirements than IT systems. The city may manage its own networks and information systems. But for maximum security, a single framework should address the management of cyber risk across the enterprise, including all utility and city departments.

**4. Do your cyber controls cover data handling and hardware/software of your third-party suppliers?**

Utilities are particularly dependent on third-party suppliers and vendors. Often, cybersecurity controls are not extended adequately into the operations of data handling or hardware and software of the vendors. When negotiating contracts, follow these guidelines:

- Incorporate cybersecurity requirements into your RFPs as contractual commitments
- View third parties as "untrusted" – specific access control required

- Request that the third party sign your cybersecurity policy or ensure they can comply with your security standards outlined in the contract
- Ensure that proper notification, respond and recover processes are in place
- Request regular cybersecurity reporting from the third party
- Request the right to audit the vendor's cybersecurity procedures and/or premises

5. **Have you allocated sufficient resources to design, deploy, and maintain your cybersecurity program?**

   To allocate sufficient funding and personnel to cybersecurity, you must understand your current vulnerabilities and security improvement needs. You may require an independent consultant to conduct an evaluation. For example, as the services organization dedicated to enhancing the performance of community-owned utilities, Hometown Connections helps utilities close cybersecurity gaps. Its low-cost **Cybersecurity Assessment** identifies improvement opportunities in cyber defenses and helps utilities develop strategies and budgets to deploy them.

6. **Are your cybersecurity policies and practices well documented, with roles and responsibilities clearly established?**

   To be effective, each cybersecurity program must emphasize that policies and procedures are as important as equipment or software improvements. Utilities and city governments must document who is responsible for which cyber defense activities.

7. **Do you provide cybersecurity awareness training to your new and existing staff on a regular basis?**

   Never underestimate the human factor in cybersecurity. Developing appropriate policies and procedures for employees and contractors is just as important as making equipment or software improvements. Only repetition can thwart bad habits and inattention. Each cybersecurity program must include training, retaining, and testing on a regular basis. Every organization must review the rules and procedures over and over again.

8. **Do employees ensuring cybersecurity compliance have adequate skills and knowledge?**

   Personnel involved in developing and managing a cybersecurity program should include key cyber risk stakeholders from the various business units in the organization. The program requires knowledge and skills in several key areas:

   - IT or network information architecture
   - Operations technology architecture
   - Risk management/insurance
     - Someone must identify, quantify, and manage cyber risk mitigation as it applies to the purchase of insurance policies.
   - Compliance or privacy

    - The legal department must track a patchwork of privacy and cybersecurity regulations by NERC, FERC and the states, as well as address contract liability issues when dealing with third-party vendors.
- Human resources
    - For managing cybersecurity training and policy compliance
- Executive sponsor, often the chief financial officer
    - The CFO must understand the economic impact of cyber risk mitigation and manage network security professionals and insurance policies.

**9. Is a senior executive driving cybersecurity as a priority across the enterprise?**

Because the organization must establish and maintain a culture that prioritizes cybersecurity across the enterprise, there must be an executive sponsor from senior management. Often the general counsel or chief financial officer takes charge of the cybersecurity program development—someone of a very senior rank who must own the strategy and drive cultural change. However, even if the general counsel or CFO takes charge of the cybersecurity effort, the utility general manager or the city manager must maintain overall accountability for the cyber program to ensure effective governance and roles/responsibilities remain clear.

**10. Is your cyber program part of a broader risk management effort?**

Cybersecurity is only one element of managing risks to business operations. To mitigate potential disruptions and minimize inefficiencies, each organization should evaluate its business practices in all areas of operations to include finance, customer service, support services, compliance, internal controls, project management, program management, training, safety, prioritization, strategic planning, governance, IT processes, information protection and safety, purchasing, vendor management, leadership, employee development and culture. Hometown Connections consultants help community-owned utilities apply risk management principles to all business operations to maximize performance and productivity.

**Learn More**
For more information on cybersecurity strategies for community-owned utilities, see these articles:

Cybersecurity Starters Guide for Utilities
Cybersecurity FAQs
Gather Information Before Engaging Cybersecurity Consultant

To learn more about cybersecurity requirements and solutions for community-owned utilities and city departments, send an email to info@hometownconnections.com.