**www.hometownconnections.com**

12081 W. Alameda Parkway, # 464
Lakewood, CO 80228

P — 970 682 4217

Hometown
Connections

# Cybersecurity Assessment Solution

## By Hometown Connections, Inc.

From Cybersecurity Management Program For Community-Owned Utilities and City Governments

# Contents

# PUBLIC POWER CYBERSECURITY MANAGEMENT PROGRAM

## Comprehensive Cybersecurity for Utility & City Departments

Cybersecurity is a significant and growing threat for all critical infrastructure sectors, with electric utilities facing extreme risks. Utilities must defend against criminals stealing information and extorting them for financial gain as well as nation states or terrorist groups seeking to sabotage information systems that operate critical infrastructure. Bad actors intent on harm include highly sophisticated organized crime networks.

Today, community-owned utilities and city governments are targets of ransomware and other attacks at an alarming rate. Data theft and service outages from a cyber attack cause great operational, financial, and reputational harm. No utility or city is too small to be targeted and no network—no matter how large and well-resourced—is completely secure.

Due to the multifaceted and ever-evolving cyber threat, electric utilities of all types must access cybersecurity expertise and solutions. Cybersecurity services are available from a variety of regional and national sources, but those resources can be expensive or not ideally suited for the typical public power utility. The policymakers and senior managers of these utilities are looking for support identifying cyber defense weaknesses AND deploying new security measures at a reasonable cost.

To meet public power's need for cybersecurity solutions that are comprehensive and cost effective, Hometown Connections, Inc. (HCI) has launched a **Cybersecurity Management Program** for public power electric, gas, water, and wastewater utilities and other city departments. A non-profit services organization for community-owned utilities, HCI is owned by public power and works on cybersecurity in close coordination with the American Public Power Association. HCI is helping public power utilities across the United States evaluate their cybersecurity requirements, develop plans for cyber risk management, and deploy effective cybersecurity defenses that include ongoing monitoring, remediation, training, and maintenance.

## Cybersecurity Assessment with Detailed Recommendations

One feature of the Cybersecurity Management Program is HCI's **Cybersecurity Assessment** service that helps public power information technology, operational technology, and utility management professionals identify their organization's cyber vulnerabilities and design a detailed cyber defense program based on industry standards and best practices.

The foundation of each utility's cyber defense strategy must be a snapshot of its current security posture. HCI works with utility personnel and their third-party providers onsite at the utility/municipality or remotely to create a cybersecurity profile. Then, HCI analyzes the information and delivers a detailed report with recommendations for how to address deficiencies, prioritize action items, and budget for security improvements.

To make sure the service is affordable to public power utilities of all sizes and budgets, the pricing for the Cybersecurity Assessment ties to the staffing, infrastructure, and network footprints of the utility or city.

# ASSESSMENT OVERVIEW

The Cybersecurity Assessment from HCI provides a snapshot of a utility's security posture. HCI utilizes several public power and industry tools to deliver a thorough, consistent analysis that results in a roadmap for next steps and budget implications.

## Deliverables for Utilities

Upon completion of the assessment, a utility will have:

- An understanding of the utility's cybersecurity maturity benchmarked with other public power utilities.
- A report on how well best practice guidelines are currently deployed within the utility's network(s) as it relates to the CIS controls and APPA scorecard.
- A list of vulnerabilities and critical systems that are exposed.
- A better understanding of Cyber Incident response and a playbook for building / improving upon this important area.
- A short-term (0-9 months) and longer-term (9-18 months) roadmap for remediation priorities along with budget costs.
- Results from phishing/cyber awareness exercise.
- An understanding of the current security and recoverability processes along with recommendations for areas of improvement.
- A report and presentation that can be shared with leadership summarizing all of the aforementioned areas.

## Utility Requirements

- The cost for this assessment is determined by a short scoping questionnaire/call.
- The utility must provide network security device configurations for all in-scope firewalls, routers and access control devices. These configurations will be held in strict confidence and will be reviewed as part of the assessment.
- The utility must agree to a vulnerability scan of its corporate IT systems. The utility can opt-out of scanning sensitive networks (ie… Industrial Control Systems, SCADA) if desired.
- A utility must produce a list of all internet connections, so that the list can be included in an external vulnerability scan. If one is not available, HCI can assist the utility in identifying these items.

# ASSESSMENT PROCESS

The HCI Cybersecurity Assessment consists of three phases.

## Phase One – Kickoff & Data Collections

In phase one, HCI holds a short kickoff call prior to the data collection activities. The kickoff call covers the following areas:

- The sensitivity of the information collected and produced, storage of the data, and how it will be transported and secured.
- The people who will be involved from the utility, with HCI ensuring all key personnel are identified and involved in the process.
- A review of schedules to determine the best dates for subsequent meetings/work sessions.
- An overview of the American Public Power Association's Cybersecurity Scorecard and obtaining the utility's commitment to complete the Scorecard by a date certain. This discussion can include determining if the utility needs assistance completing the Scorecard and what business areas (e.g., electric utility only, other city utilities, the city, etc.) will be part of the assessment.
- An overview of the Center for Internet Security (CIS®) Critical Security Controls (CIS Controls) to understand what it is, how it will be used, and what to expect from it.
- Discussion of IT versus OT networks and a determination of what systems will be out of scope for the engagement or portions of (e.g., vulnerability scan).
- Review of data needed from utility. Examples include: configurations from all the utility's firewalls, routers and access control devices, IT policies, IT staffing/org chart, current and projected IT budget, system architecture and any applicable diagrams, a list of the utility's internet connections and known IP addresses, and any previous assessments performed by or for the utility and arrange for that information to be shared with HCI prior to the assessment. HCI will review one prior assessment up to 50 pages in length.

## Phase Two – Remote and Field Work Activities

Phase two begins after all data is collected from phase one. Phase two includes:

- Calls to review and ask questions about collected information from phase one.
- Scan external IP addresses to collect data regarding the utility's internet footprint.
- Scan of internal in-scope network(s).
- Collection of an Incident Response Plan and a Disaster Recovery Plan, including any associated policies.
- Review of IT budget, and any current and future IT projects.
- Completion of phishing / cyber awareness exercise.

## Phase Three – Share Results

In the final phase the overall results of the assessment will be shared, along with a review of the American Public Power Association's Cybersecurity Scorecard. These recommendations include:

- Identification and prioritization for remediation of the issues discovered.
- Associated suggestions for any tools, services or other means for correcting the identified issues.
- Budgetary estimates (and suggested prioritization) of these recommendations.
- Recommendations for improving an Incident Response Plan or the groundwork for creating one.

- Recommendations based on the review of a Disaster Recovery Plan.
- A review of the CIS Controls that were graded along with pragmatic recommendations for application of missing controls.
- Phishing/security awareness exercise results will be shared with the utility and any training opportunities identified.
- Share final report and presentation.

## JOINT ACTION AGENCY PARTICIPATION

Public power joint action agencies may arrange a purchase of HCI's Cybersecurity Assessment service on behalf of their members, to secure group savings and deployment efficiencies. In addition, HCI can arrange for JAA personnel to conduct elements of the assessment on site at their member organizations.

## FOR MORE INFORMATION

Contact Hometown Connections for more information on the Public Power Cybersecurity Management Program and its Cybersecurity Assessment service:

Hometown Connections, Inc.
12081 W. Alameda Parkway, # 464
Lakewood, CO 80228
Phone: 970-682-4217
Email: info@hometownconnections.com
www.hometownconnections.com