



CLIENT FACTS

BUSINESS NEED

To meet requirements of NERC Critical Infrastructure Protection (CIP-014) Compliance

BUSINESS SOLUTION

Security and Compliance Risk Compliance solution using SecureWatch by RiskWatch International

BUSINESS VALUE

Objective and expert physical security and compliance audit identified high risk facilities who received priority on-site risk assessment and an actionable roadmap for meeting CIP-014, including R4 and R5 and reducing security risks.

To meet requirements of NERC Critical Infrastructure Protection (CIP-014) Compliance, our client needed a solution that would allow them to perform assessments that would efficiently and effectively gather data needed for compliance, categorize data and view risks throughout their service territory while providing auditable evidence for 3rd Party reviews and Auditors.

ABOUT CLIENT

Our client is a Fortune 500, diversified energy company. Its subsidiaries and affiliates are involved in the generation, transmission, and distribution of electricity, as well as energy management and other energy-related services. Its ten electric utility operating companies comprise the nation's largest investor-owned utility, based on serving 6 million customers within a 67,000-square-mile (170,000 km²) area of the north eastern US, covering multiple states. Its generation subsidiaries control more than 23,000 megawatts of capacity, and its distribution lines span over 194,000 miles.

SITUATION

Our customer set out to improve their Physical Security Risk Assessment program to meet CIP standards. Realizing that any activity within their generation, transmission, and distribution of electricity could impact their service territory, they determined they would need greater visibility of their sites while maintaining a risk score card at each in order to meet and achieve compliance. Some of these goals included reducing cost of detailed on-site assessments, assessing threats and identifying vulnerabilities across the organization, mitigating potential threats or vulnerabilities all while building the information that is needed for CIP-014 Compliance and/or audits.

The challenges the customer faced were multi-fold:

- How to assure senior leadership that security measures are in place to protect employees, preserve critical assets, meet compliance and enable continued growth?
- Evaluating Security controls in place and how these might be leveraged to ensure compliance and meet all the requirements of CIP-014, including R4 and R5.
- How could the company efficiently gather security data from multiple sites so they could track and manage the changing security profile?
- How could the company efficiently process the data to drive decision-making while also keeping one step ahead of potentially damaging activities?
- How could they provide auditable assessment evidence and resolution of risk or vulnerabilities identified?
- How could they use assessment data to standardize the assessment process to save the time required to populate an assessment with relevant data that is required for the assessment?

SOLUTION

- RiskWatch International's, SecureWatch™, provided a dynamic solution to help the customer undertake a Physical Security Risk Assessment program that included a Preliminary Risk Assessment that provided Risk Scores for each facility (based on threats, vulnerabilities, and facility criticality).
- Provided a solution with pre-loaded standards, security plan and audit-ready reports that will help them meet all the requirements of CIP-014, including R4 and R5
- Facility managers were provided access to a portal for surveys and uploading assessment data that allowed them to access reports and a risk scorecard for their facility.
- The critical facilities associated with High Risk received priority and were scheduled for an on-site detailed risk assessment. The assessment encompassed a wide range of data, including safety & security violations or incidents, internal and external threats & vulnerabilities and 3rd party intelligence sources.
- Security managers could access a Risk View that categorized risks throughout the service territory into a matrix at a high level but still allowing them to drill down to see vulnerability that was associated with the risk, any remedial efforts currently taking place and how that risk will improve as efforts are completed.
- Risk View allowed the customer to provide auditable evidence for 3rd Party reviews and Auditors.
- Data registers and third party data providers were used to populate new assessments with standard sets of data and previously completed assessments were used as templates for assessments at similar facilities, saving time required to gather and populate assessments with data needed to complete the assessment.
- Assessments could be assigned by security managers to be performed by security personnel or facility managers and then later analyzed by security managers.

RESULTS

Utilizing SecureWatch, the customer:

- Achieved significant security improvements and compliance with NERC CIP-014 standards by assessing facilities and service territories in a solution built around CIP standards.

Saved time and money performing assessments:

- 70% of time performing assessments was saved when assessments were conducted from data registers.
- 80% time saved when assessments were conducted from previous assessments performed in SecureWatch compared to their previous manual assessment process.
- Overall assessment results effectively communicated the state of facility security to all business stakeholders through a security risk rating for individual facilities.
- Increased visibility and transparency with facilities, enabled the customer to make more insightful decisions—decisions that were driven not just by price, but also guided by an understanding of the potential risk and vulnerability that a “High Risk/Critical” facility posed.
- Utilizing both internal and external data collection, the company was confident that they had access to a complete picture of its facility physical security.