WE
Western Energy™
The Official Publication of
Western Energy Institute

CULTURE SHIFT:
Risk Management is Everyone's Responsibility

Indoor Agriculture and Energy Implications

Leak Management's Role in Safety and Reducing Risk

Partnering with Outside Organizations for Enhanced Cybersecurity

RISK ASSESSMENT
Processes, People + Systems

HYDRO OTTAWA
Creating a Road Map for Investing In Utility Infrastructure

PARTNERING WITH OUTSIDE ORGANIZATIONS FOR **ENHANCED CYBERSECURITY**

By Neil Neroutsos, Snohomish County Public Utility District

An unfortunate reality in our modern world is that hackers routinely attempt to wreak havoc on our computer information systems. In recent months, numerous corporations have been targets, including Target, Sony Pictures and Premera Blue Cross.

The United States' electric grid also is a primary target. In a briefing before a Congressional committee last fall, the National Security Agency alerted legislators about the concerted efforts by foreign hackers to use malicious software to infiltrate, and potentially cripple, critical infrastructure, including the nation's electric grid.

Snohomish County Public Utility District (PUD), north of Seattle, has taken proactive steps on several fronts to enhance its security measures. In recent years, it has partnered with other utilities, and public and private organizations to organize cybersecurity summits to identify threats and share response plans.

Earlier this year, the utility worked with a Washington National Guard team to assess the PUD's cybersecurity defense as part of a groundbreaking, two-week "penetration test." It was the first such operation ever conducted by a National Guard team. During the exercise, the team attempted to attack utility systems, including operational systems such as substation controls, and administrative systems, such as human resources and customer service.

The National Guard's operation proved invaluable, because it helped better identify the types of risks the utility should be looking for from hackers. During the simulation, the PUD also learned ways to fine tune its response processes if and when an actual cyberattack occurs.

"Electric utilities need robust response and recovery plans that include the sharing of information and other mechanisms to protect against cybersecurity events," said PUD Chief Information Officer Benjamin Beberness. "The National Guard team's expertise was top notch, and the output will help the PUD improve its response and recovery plans."

Most utilities use tabletop exercises to test cybersecurity response. According to Beberness, penetration tests take it to the next level by exposing weaknesses in the plans, since they test actual detection and responses to attacks in real time. In the PUD exercise, a smart-grid test lab was used to mirror actual systems from EMS/SCADA and substations, to battery storage devices and distribution automation systems.

In order to respond to a cyber event, the PUD has to be able to detect the event. To help the PUD test its detection capability, the team knew that the Guard's attack would come during a two-month window, but it didn't know the actual timing or what means would be used to penetrate the utility's systems. This provided a better test of the PUD's detection capabilities.

The Guard is looking at ways to replicate the penetration test for other utilities and critical infrastructure around the country. These operations have significant value, particularly for smaller utilities that may not have the same levels of security and funding to pay for these exercises.

Beyond such exercises, educating utility staff also is essential. PUD employees receive training to ensure that they're aware of potential hacking scams and what steps are needed to safeguard the integrity of the utility's systems. For the PUD, cybersecurity is fundamental to its business operations. It invests time and resources in order to continuously monitor and prepare for constantly evolving cyber risks.

Q+A with Benjamin Beberness, Chief Information Officer

WHY DID YOU START YOUR UTILITY'S CYBERSECURITY PROGRAM?

All utilities face risks from hackers and other cybersecurity threats. Utilities need to consider if they're taking all necessary measures to protect their systems. At Snohomish PUD, we've developed a cybersecurity program as part of our Smart Grid Investment Grant from the U.S. Department of Energy. It includes a set of security controls, lays the foundation for a cybersecurity risk management framework, and provides education and awareness for our employees. Snohomish PUD always has taken cybersecurity seriously and we understand that we need to continuously be aware of the evolving cyber risks.

WHAT HAVE YOU DONE SO FAR?

Snohomish PUD employees are required to take regular, online training courses to alert them to the latest scams and give them the tools they need to protect our systems. The utility also participates in several national forums with organizations such as EnergySEC, the Large Public Power Council, American Public Power Association, Western Energy Institute and others. We've worked with other Northwest organizations to hold two cybersecurity summits, where we shared information and briefed congressional staff and other government officials. We've also participated in emergency exercises, organized by the Department of Homeland Security and the U.S. Department of Energy, which simulated cyberattacks and tested our level of response. The utility also has formed a Cybersecurity Steering Committee, comprised of its senior leadership.

HOW HAVE YOU SEEN IT BENEFIT THE UTILITY?

As a region, we've benefited by sharing cybersecurity best practices among public agencies, such as the City of Seattle and the National Guard, and major corporations, such as Microsoft and Amazon. Through our participation in regional and national cyber events, we've identified areas for improvement. Internal communications, for example, have improved as we learned how, what and when to communicate cyberattack information to outside authorities, and among our internal divisions. Increased employee awareness has been central to our program.

WHAT ADVICE DO YOU HAVE FOR OTHER UTILITIES ABOUT STAYING ON TOP OF CYBERSECURITY?

The active involvement of a utility's senior leadership, information sharing and communication components are critical. Utilities need robust response and recovery plans to protect against vulnerabilities. Smaller utilities with limited resources should consider adopting the U.S. Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model, which is risk-based and allows a utility of any size to focus its resources on its highest risk.

NEIL NEROUTSOS is media liaison for Snohomish County Public Utility District, which serves 333,000 customer accounts north of Seattle, Wash.