Case Study

Cybersecurity Transformation In Rural Electricity

Situation

One North American Electric Cooperative initiated an ambitious transformation of its IT and Operational Technology (OT) systems. The Cooperative needed to align its infrastructure with the focus on newer technologies while meeting the cyber security objectives set by the National Rural Electric Cooperative Association (NRECA) Rural Cooperative Cybersecurity Capabilities program (RC3).

The rapid transformation of the energy landscape towards renewable sources presents a new set of cyber security challenges, especially for rural electric cooperatives. These cooperatives play a vital role in distributing power to rural and remote regions, making their security paramount.

Challenges

The Cooperative considered the following challenges when building their cyber security roadmap:

New Software and Networks: Integrating new software and hardware into existing systems to enhance communications and operational networks brought substantial benefits. However, it also introduced fresh vulnerabilities.

Remote Support: While new support mechanisms improved troubleshooting and maintenance, they also expanded remote access, exposing substation systems to new threats and potential intruders with network access and passwords.

Solution

As an established global expert in cyber security consulting and risk mitigation, NCC Group was primed to guide the Cooperative through this intricate transformation.

The Group's Facility Due Diligence service, led by Jim Mckenney, Practice Director for Industrials, was integral to the initiative.

Harnessing the strengths of the Validated Architecture Design Review (VADR) methodology, NCC Group tailored an approach to address the unique needs of the Cooperative.

The journey began with a thorough review of the Cooperative's main offices and industrial control facilities. NCC Group's team worked meticulously, unraveling a complex set of vulnerabilities that could potentially compromise their critical systems. Notably, the Cooperative was unknowingly allowing unauthorized access to their Energy Management System (EMS) and Distribution Management System (DMS).

These systems play an instrumental role in the transmission,distribution, and optimization of electricity across their extensive grid. By detecting and eliminating malware presence on the Cooperative's systems, NCC Group effectively shut the door to potential third-party interference.

At a glance

Organization: Rural electric cooperative

Industry: Energy & Utilities

Situation: Securing a digital transformation initiative in alignment with the NRECA RC3 program

Challenge: New software and networks for IT/OT integration introduced fresh vulnerabilities, and expanded support mechanisms exposed remote access concerns-especially for substation systems.

Solution: Tailored cyber security consulting carried out by the Facility Due Diligence team reviewed security architecture, recommended access management systems, and delivered a full, actionable report to coop leadership highlighting critical security measures.

Results: The coop not only met the objectives of the RC3 program but also- with NCC Group's guidance- developed a 3-year roadmap to invest in the continued security and efficiency of their people, processes, and technology.

NCC Group's approach to addressing these vulnerabilities focused on collaboration. The team worked closely with the Cooperative's local field engineers, reviewing the current architecture plans, and conducting facility walkthroughs. These interactions facilitated open dialogues about discrepancies in the system architecture and the associated cyber risks. The transparency fostered a shared understanding of cyber security risks and objectives, dispelling apprehensions about potential disruptions to operations.

The assessments resulted in an actionable report matched to the Cooperative's specific needs. Key recommendations from this report included:

- Implementing a Privileged Access Management System (PAMS) to secure access to SCADA systems from the enterprise network.
- Improving mobile application security.
- Introducing multi-factor authentication for remote access.

These measures, aimed at enhancing security, also provided benefits such as improved overall system usage insights and a reduced risk of human error-induced outages.

Results

After NCC Group's efforts, the Cooperative not only met the requirements on the RC3 checklist but also provided an informed status report to its leadership. The Cooperative and NCC's collaboration led to the development of a three-year roadmap for capital investments, demonstrating their commitment to advancing cyber security. This roadmap effectively aligned cyber security requirements with proposed design changes and focused on optimizing efficiencies and processes to minimize operational costs.

The adoption of a modernized reference architecture based on the NIST Framework and Roadmap for Smart Grid Interoperability Standards and IEC/ ISO 62443 standardized the Cooperative's technology, tools, and apps into a unified pattern, enhancing the security and efficiency of the infrastructure.

The implementation of a new standardized technology architecture for the Cooperative's substations was a notable achievement in this transformation. The move from a theoretical concept to practical application was a significant step towards aligning seamlessly with operations.

> *"Our experience with NCC Group was an eye-opener. Their holistic approach to cybersecurity assessment helped us identify our vulnerabilities and provided a clear, actionable plan.*
>
> *The collaborative process bridged gaps between our IT and field teams, creating a shared understanding of our cyber security goals.*
>
> *We now have a solid foundation and a clear three-year roadmap for our cybersecurity initiatives."*
>
> - Coop Representative

The transformation was not solely focused on systems and procedures; it also prioritized people. NCC Group's cyber security training for controls and field engineers offered focused instruction on operational technology and supporting networks. It enlightened them on the signs of malware and ransomware attacks and equipped them with the knowledge to contain such incidents effectively.

Case Study

Cybersecurity Transformation In Rural Electricity

The Cooperative's transformation is a testament to the progress that can be achieved with clear focus, expert guidance, and a collaborative approach. Through this journey, NCC Group demonstrated how a deep, bespoke approach to cybersecurity can seamlessly align with operations. The transformation validates that maintaining security in the face of rapid technological advancements is achievable with the right partnership and vision.

Key Takeaways for Improved Cyber Defence

Security in electric cooperatives is paramount as they stand at the intersection of technological innovation and emerging vulnerabilities. By embracing industry best practices, these cooperatives can fortify their operations against digital threats and real-world challenges. Here are some recommendations for other cooperatives to follow:

1. **Seek Expert Guidance:** Engage established cyber security firms for guidance through complex cyber security transformations, ensuring that the transition is informed and efficient.
2. **Adopt Custom Approaches:** Use methodologies like the Validated Architecture Design Review (VADR) to tailor strategies, addressing the specific needs of each cooperative. This ensures that unique challenges are adequately addressed.
3. **Conduct Comprehensive Facility Reviews:** Regularly review both office and facility infrastructures. A deep dive into systems can unearth vulnerabilities and opportunities for system optimization.
4. **Prioritize Vulnerability Detection:** Invest in tools and expertise to uncover and address vulnerabilities, particularly unauthorized access to critical systems. Early detection can prevent impactful breaches.
5. **Champion Collaborative Strategies:** Foster a culture of collaboration, working closely with field engineers and stakeholders. Engaging all members can lead to more effective and holistic solutions.
6. **Generate Actionable Reports:** After any cyber security assessment, create specific and actionable reports. These ensure that insights lead to practical measures that can be implemented for improvement.
7. **Plan for the Future:** Create roadmaps for capital investments in cyber security. This forward-thinking approach ensures cooperatives stay ahead of emerging threats and capitalize on new opportunities.

NCC Group Cyber Security in Energy RC3 Program Assistance

Rural Cooperative Cybersecurity Capabilities Program (RC3)

At NCC Group, our Cyber Security Facility Due Diligence Program is specifically crafted to swiftly, efficiently, and cost-effectively address the distinct tech challenges faced by rural cooperatives.

As they work towards the 10 RC3 Objectives outlined by NRECA, we draw from industry best practices to guarantee personalized expertise tailored to each cooperative's unique requirements.

The objectives we focus on include:

1. **Cyber security Contact:** We set up a dedicated individual to handle all your cyber security concerns.
2. **Self-assessment:** Our team assists in a thorough review of your current cyber security infrastructure.
3. **Contract Review:** We'll scrutinize your contracts, ensuring they have strong security provisions.
4. **Multi-factor Authentication:** We guide the setup of layered security access for enhanced protection.
5. **Password Standards:** With us, you'll establish robust password protocols to keep threats at bay.
6. **Leadership Involvement:** We stress and support a top-down approach to cyber security.
7. **Employee Training:** Benefit from our direct training sessions, sharpening your team's cyber security acumen.
8. **Separating IT and OT:** We'll advise on cleanly segregating standard and operational tech to minimize risks.
9. **Incident Response Plan:** Together, we'll craft a solid plan for any potential cyber security incidents We also provide affordable Computer Incident Response Retainers for both Enterprise and OT networks and systems.
10. **Data Backups:** We'll ensure that your crucial data is backed up and secured regularly.

With NCC Group, cooperatives are equipped to navigate the digital transition seamlessly and securely.

Power your security strategy with expert-led review.

To learn more about NCC Group’s RC3 Program Assistance or our other products and services for the Energy & Utilities sector, please get in touch at nccgroup.com/contact-us