COALFIRE

CASE STUDY

NISC leverages Coalfire-authored white papers to help members understand how to validate their PCI DSS compliance

AT A GLANCE

National Information Solutions Cooperative (NISC) is an information technology cooperative that develops and supports software and hardware solutions for utility and telecommunications cooperatives and companies (i.e., members/owners) across North America. As a leader in the electronic payment space, NISC develops solutions to make payment processing simple for members.

CHALLENGE

"Today's customers require more flexibility in the way they choose to pay," explained Mike Coumerilh, information security consultant at NISC. "Our members have their choice with a vast variety of payment solutions depending on their customers' needs." When members inquired about which self-assessment questionnaire (SAQ) to fill out or how to respond to a particular question, NISC would answer to the best of its ability with its limited understanding of the member's particular environment. "We would refer them to the Payment Card Industry Data Security Standard (PCI DSS) requirements and security assessment procedures PDF or First Data, their acquirer, for support," says Coumerilh. "It was difficult to differentiate some concepts that were similar but different. Because of this, there were complaints of conflicting answers to questions and an over-complication of details to make distinctions between two words or ideas."

To reduce confusion and uncertainty surrounding members' PCI DSS requirements, NISC developed an initiative to partner with an independent third party with ample PCI experience and a credible name in the marketplace. The purpose was to help increase understanding of where PCI DSS requirements were applicable to various member business environments and also how to demonstrate PCI compliance when answering applicable requirement questions. After a comprehensive decision-making process, Coalfire was ultimately chosen based on their PCI compliance expertise, experience writing objective product applicability guide white papers, and their ability to understand and provide a beneficial solution to fit NISC's needs.

"Coalfire came recommended by one of our members, and after speaking with them, we felt their solutions would aid our objective of effectively communicating the importance of validating PCI compliance," says Coumerilh.

APPROACH

Coalfire reviewed NISC's initial requirements and ensured they were realistic and sufficient. Using security best practices and customized testing methodologies, Coalfire evaluated each solution against NISC's claims of capability to address key compliance objectives. Coalfire reviewed documentation and interviewed subject matter experts, solution architects, developers, and other key stakeholders to confirm the functionality of the applications and their implementation within the PCI DSS environment. The NISC's solutions were set up in a lab environment for various deployment scenarios. The assessment included a comprehensive set of administration, technical, and physical control testing performed for the deployment architecture.

Coalfire validated the solutions by testing the supported applications with the use of integrated pin-pad terminals, monitoring the transactions to confirm data flow, and ensuring guidelines were noted within the implementation guide for customers. NISC applications software development lifecycle (SDLC) processes, secure coding practices, change control procedures, and vulnerability management processes were reviewed and confirmed to follow the necessary standards.

Coumerilh stated, "Many times, industry experts come in with such authoritative control that they dominate the engagement and leave little room for dialogue, or they leave their expert opinion at the door and fail to ask enough investigative questions to fully understand their client's most basic requirements. Coalfire is neither of these. Coalfire knows how to build a relationship as a true consultant, engaging with us to understand exactly what we are looking for and meet – or help us to adjust – our expectations. In addition, we were impressed by Coalfire's shared history and existing relationship with First Data and were pleased with First Data's acceptance of the white papers as an authority for NISC's card payment solutions' PCI DSS scope for our members."

RESULTS

NISC is now able to clearly delineate their (merchant) responsibility, and members can clearly identify their PCI scope with more confidence, which translates into higher engagement numbers, less risk, fewer questions to their business, and less time spent addressing concerns.

"We now have companion white papers for our most-common member environments that enable members to go from start to finish with a synergistic path to validate their PCI compliance," says Coumerilh. "Our Coalfire-authored white papers helped us strengthen our position as PCI DSS industry experts with our members and prospects. They provided us with relevant knowledge and expertise to guide our members through incorporating PCI compliance into their overarching security processes, or to use them as a foundation to build upon. We have also been able to take what we have learned and improve our overall cybersecurity strategic initiative both internally and for our members."

COALFIRE

About Coalfire

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com.**

CS_NISC_111419