River City Bank

RIVER CITY BANK'S DATA VAULTING JOURNEY TOWARDS SHELTERED HARBOR CERTIFICATION

- Institution: River City Bank
- Headquarters: Sacramento
- Size (range): $4.3 Billion
- Accounts Protected (deposit, brokerage etc): Deposit
- Time from Program Inception to Certification: 6 months
- Lead in organization: Matt Huber, SVP Director of Operations, River City Bank
- Team composition and headcount: Banking, Security, Data Governance, Banking Operations, Vendor Management, Senior Leadership, Technology Services, Project Managers

OVERVIEW

River City Bank, founded in 1973, has evolved into the premier business bank in the Sacramento region, with assets exceeding $4.3 billion. It's the largest, independent, locally owned, and managed bank in the Sacramento region, with offices in the San Francisco Bay Area and has a presence in Southern California. Recognizing the growing importance of cybersecurity, River City Bank embarked on a mission to enhance its cyber resilience. In this case study, we explore how River City Bank leveraged Sheltered Harbor, the financial industry's cyber resiliency initiative, to achieve Data Protected Certification and to fortify its defenses against potential cyber threats.

PRIOR TO SHELTERED HARBOR

The Sheltered Harbor approach of focusing on the core data and using a standard file format that every financial institution would adopt appealed to River City Bank. They equated adopting the Sheltered Harbor approach to an insurance policy for their

Business Continuity and Disaster Recovery (BC/DR) plan. They believed the Sheltered Harbor Solution fit well within the BC/DR by providing a roadmap for cyber-resilience as well as aligning with regulatory expectations. It was important to them to stay ahead of what the regulators may require in the future.

EXECUTIVE-LEVEL BUY-IN AND PRIORITIZATION

The risk management department and the Bank's IT Director advocated for the adoption of Sheltered Harbor. With their recommendations, the approval process swiftly gained traction, especially since the bank's C-suite executives sit on the bank's risk management committee. Understanding the importance of cyber resilience, the implementation of the Sheltered Harbor solution was given a high priority.

STRUCTURING THE IMPLEMENTATION WITH EXTERNAL SUPPORT

River City Bank's smaller size and limited bureaucracy made it easier to streamline the implementation process. The project brought together the IT and Operations teams, who collaborated closely to ensure a successful implementation. River City Bank sought the expertise of FIS, a reputable technology solutions provider, to assist with the implementation of Sheltered Harbor. FIS acted as a reliable partner, offering step-by-step guidance, and ensuring the bank's successful adoption of the initiative and achieving certification. Regular update calls with FIS, helped keep the bank on track as it progressed towards certification.

PROCESS HIGHLIGHTS

FIS played a pivotal role in guiding River City Bank through the implementation process, providing a structured approach and a clear set of six key tasks to complete. The bank's primary goals during this process were to achieve certification and vault its critical core deposit data securely.

As early adopters, the River City Bank team got involved in several of Sheltered Harbor's discussion groups including the Registry and Resilience Discussion Groups. The discussion groups are composed of Sheltered Harbor participants and subject matter experts who help shape the direction of all aspects of the initiative, from technology to adherence to communications to regulatory relations. Even though the

initiative is far more mature than in the early days, the team believes that getting the context of how actions are progressing is helpful to any participant. They also encourage all participating financial institutions to work closely with the Sheltered Harbor team while using the valuable guides that take you step by step through the process.

TECHNOLOGICAL CONSIDERATIONS AND CHALLENGES

River City Bank faced certain technological challenges during the implementation. One issue involved a few data fields that were not correctly pulled from the bank's core processor. Resolving this discrepancy required time and effort. Additionally, the bank had to create its own queries to validate and verify customer data, as there was no standard report available from FIS for this purpose. River City Bank utilized FIS Business Intelligence Center (BIC) software, but they had to develop their own custom reports to ensure data accuracy, relying on queries to validate information.

PREPARING FOR A POTENTIAL DOOMSDAY

River City Bank dedicated approximately six months towards vaulting their data. The bank's focus during this period was on learning how to validate the file and ensure a straightforward and efficient process. The validation stage posed the most significant challenge, but with the assistance of the FIS team, River City Bank overcame obstacles and developed a deep understanding of the data involved. The bank performed spot checks on specific customers, wrote custom reports, and utilized FIS's BIC software to validate and verify information accurately.

CONCLUSION

River City Bank's journey towards cyber resilience through Sheltered Harbor demonstrates its commitment to safeguarding customer data and fortifying its defenses against cyber threats by protecting their critical customer account data. By partnering with FIS and following a structured implementation process, the bank successfully achieved Data Protected Certification and established the beginnings of a robust cyber resiliency framework. River City Bank's proactive approach towards vaulting the critical data sets exemplifies its dedication to providing a secure banking experience for its customers and ensuring the integrity of its operations.