SHELTERED HARBOR CASE STUDY

FIRST BANK: THE EARLY ADOPTER

- Institution: First Bank
- Headquarters : Denver, CO
- Assets : $19 billion
- Accounts Protected: Deposit
- Time from program inception to data vaulting: 12 months
- Team: Albert Kendrick - First Bank CIO , Brian Dennehy - Senior Director IT , Travis Knox - Senior Security Analyst , Jon Schow - Senior System Administrator.

OVERVIEW

First Bank's adoption of Sheltered Harbor stems directly from its determination to stay on top of trends in the financial services industry. "We need to keep our hands in all the changes going on in the industry, so we know where to focus and invest," says CIO Albert Kendrick. From active participation in industry associations like the American Bankers Association (ABA), to early adoption of Zelle and The Clearing House's (TCH) Real Time Payments network and participation in the Federal Reserve's Faster Payments Task Force, First Bank (FB) sees itself as an innovative tech-forward bank that operates more like an institution with $30-50 billion in assets than its $19 billion.

In addition, First Bank places a high priority on security and incident response."Security is not a check-off item; it's a strategic enabler. If we can do security well, then we can be aggressive in a lot of areas of our business, like payments or products." Developing that reputation means that all stakeholders, from internal and external auditors to examiners to their board, have confidence when it comes to implementing technology programs like Sheltered Harbor. "We get a lot of yeses because of our approach. That means we can pursue opportunities that otherwise we would have gotten a lot of pushback on."

So when the ABA approached FB's COO, now CEO Jim Reuter, to be one of Sheltered Harbor's first smaller-sized participants, it was an easy decision. Both Reuter and CIO Kendrick were in, and their buy-in made its implementation an easy sell to FB's board of directors. "We went to our board and said, 'We're going to aggressively pursue this. We're opting to be a leader rather than a follower here or even in the middle of the pack,' and they were supportive."

First Bank took an aggressive approach to implementation, and became one of the first participants to achieve Sheltered Harbor SET status. As one of the first movers, here are some of the lessons they learned.

EXECUTIVE BUY-IN

When seeking approval from the Board, Kendrick did not have a specific budget, but he knew it would be within his decision-making authority as CIO. That executive-level prioritization is a key to their early success with Sheltered Harbor. "The CIO is the lowest level you have to have some buy-in to really get it moving," says Kendrick.

"I helped make it a priority in terms of development efforts. It would have been a lot more difficult for someone pushing from a lower level."

CROSS-FUNCTIONAL TEAM

Kendrick asked one of his senior IT leaders, Brian Dennehy, to put together the team and resources. Dennehy put together a small core team with key competencies: security, systems administration and automation, software development, project management, and audit.

Bringing in an audit from the beginning was a strategic decision by Kendrick. "If you know you're going to get graded and you can get someone to tell how you're going to be graded, bringing them along for the ride is a good way to make sure you get an A," says Kendrick. "We wanted to make sure this was a partnership, not something that was reviewed after the fact."

Sheltered Harbor takes a relatively hands-off approach to audits. "The spec just says you need to, but they don't tell you how to do it," says Senior System Administrator John Schow. Because the audit team built the program from the ground up, it was even more important for them to be involved early on. "That was a good move, doing it early on. It's what's helped us be as successful as possible."

PROCESS: UPFRONT EFFORT, ONGOING MAINTENANCE

First Bank implemented Sheltered Harbor in about six months. "We chewed through the requirements at the rate of about one a week." The team used the agile approach to project management, broke it up into pieces, divided and conquered, then reconvened to chain the pieces together. They spent time up front with the specification to figure out what decisions needed to be made, what the pieces were for both implementation and ongoing program maintenance, looked at what they already did and didn't have in place, and then also spent a lot of time on security and compliance.

"Spend a good amount of time getting into the details of the specification and put together a workflow of what you need to do," says Schow. "When you put your plan together, realize it's not a build-it-and-forget-about-it process, it's ongoing. There will be a lot of effort initially, getting it to production and making sure it works, and then things will slack off over time. But you do need to come back from time to time, re-visit the specification and see how it's changed, and determine if you need to make some changes to your own internal process."

WHEN TO UPGRADE VERSIONS

Sheltered Harbor's deprecation policy is that institutions implement the version that is current at the time they begin implementation. They will receive notice six months before the version they implemented is to be deprecated, and once it is, they have two more years to upgrade to the current version.

"If you go down the road of Sheltered Harbor, odds are good that the spec will update while you're still in the process. I would recommend taking the current specification and planning to use that to take everything into production regardless of the changes that come out in future documents,"says Schow.

However, Schow also says that it might save you work to have a look at version updates that happen while you're in the midst of the process. "Keep an eye on the things that have changed. If there's something that makes your implementation a lot easier, it might be worth changing."

USE SHELTERED HARBOR GUIDES

"It was fun to come up with solutions, to set the tone within the Sheltered Harbor community," says Dennehy. But being such an early adopter means that their program knowledge is concentrated in the heads of the original team. "It's simple for the people who know it, but if Jon doesn't show up tomorrow, I'd have to have someone go through his GitHub and figure it out. Same with Travis – he's the key to our encryption ceremony. It's that tribal knowledge that you get from being a part of it." Dennehy says he wouldn't have said no to more of a "vanilla" install, the ecosystem of partners, and the content portal full of resources now available to help participants with implementation.

CERTIFICATION

The team is now working on getting Sheltered Harbor certified, which was introduced after they'd implemented an earlier version of the spec. "It's valuable from a board perspective," says Kendrick. "Instead of us just going, 'hey, we've implemented this,' the fact that we can say we've reached this certification level says to the board that we've reached a definitive goal."

TECHNOLOGY

First Bank entered the implementation process with some advantages: they operate their own core and many systems are developed in-house, which meant they didn't have to use a core processor. "We're both smaller and less complex than the big banks, but we control our own destiny, so we can be more agile. We didn't have to engage any vendors. It was the perfect storm of circumstances; we could make it a priority with our own resources."

EXTRACTING CUSTOMER DATA

Sheltered Harbor's file structure is based on a file structure already in wide use across the industry, known as FDIC Part 360. Because First Bank was already using that file standard, "it was relatively easy. We already had Part 360 in place, we just had to augment it a bit." Originally, the team built the files once a year for their examiners, so all they had to do was set up the process to pull the files daily.

From there, the team built an FTP process to go from the mainframe to distributed servers, automated that, then had to figure out how to encrypt the data.

ENCRYPTION

"The (data archiving) process itself is simple," says Schow. "Take important customer data, make sure it's valid, track the files that go in, zip it, encrypt it, prove you've done that, store it in a write-once-read-many format, and delete when you don't need it anymore. No one of those steps is so difficult, except encryption."

"It uses AES-256 which is pretty well understood, but it uses a different cypher called GCM – and GCM behaves in a way that I wasn't familiar with." At a high level, GCM lets you perform authenticated encryption, which means you can validate that the data is the right data, without actually having to decrypt the file and look.

First Bank says they found it hard to find documentation on the GCM cypher, and products that supported AES- 256 GCM. That was further limited by some of the other software requirements for the specification.

First Bank counts itself lucky that their security SME on the team, Travis Knox, had encryption experience, but not every bank has an in-house encryption expert. "What made it easier was that I already did have prior experience in dealing with encryption key ceremonies," says Knox. "So when we had to build a process around the encryption keys for Sheltered Harbor, that knowledge was already there. It was a hurdle we didn't have to jump through."

Though the team did put it all together eventually, they still plan to make the switch to Sheltered Harbor's new encryption utility. "Rather than shop around for something that meets all the requirements of the spec, that work has already been done," says Schow. And they'll always know that piece of the puzzle will always be compliant, they'll be able to get technical support if things break, and they'll be able to compare notes with peer organizations rather than acting as a lone wolf.

VAULTING IN THE CLOUD

The next question was where the data would be stored. First Bank had several considerations in its choice: the requirements of the Sheltered Harbor specification itself; their determination that the process should be automated, and the fact that as an organization, First Bank was migrating to the cloud and away from physical storage.

Based on discussions with Sheltered Harbor and other participants, the team chose to use Amazon Glacier as their vaulting solution.

"You're shipping off your customer data, that's not something to be taken lightly. We spent a huge amount of time on security, compliance, and audit. It's a big deal to send out that data."

So the team used test data to vet every aspect of the process, all the way through getting sign off from audit and Kendrick, the CIO. Only after ironing out every wrinkle did they "turn on" actual customer data.

Looking back, the team says that one of the pieces of the process they would have gotten external help with was the AWS implementation, because it was so new to them.

CONCLUSION

As for the industry, Kendrick believes that Sheltered Harbor is a tremendous opportunity for industry to solve a problem without being forced to solve it by regulators, which he feels there hasn't been enough of. "There is a significant risk of banks being brought down from a cyber perspective – just because it hasn't happened, doesn't mean it won't. The prospects are real enough that we need to prepare."

The team at First Bank believe their hard work early on will pay off not just for them, but for their peers in the industry. "We were early adopters, and we had to figure out a lot on our own. Sheltered Harbor has made tremendous progress, it should be much easier today than it was when we started."