SHELTERED HARBOR CASE STUDY

CBC

CHARTING A RESILIENT FUTURE

- Institution: California Bank of Commerce
- Headquarters: Del Mar, California
- Size (range): 4.3 Billion Dollars, Mid Sized Commercial bank
- Accounts Protected (deposit, brokerage etc): Commercial Bank
- Time from Program Inception to Certification: 9 months
- Team Composition and headcount: 4 2 IS and 2 Operations
- Service provider: FIS

OVERVIEW

California Bank of Commerce in Del Mar, California. We're a $4.2 billion bank, commercial bank, that's our key focus.

CHALLENGES WITH RESILIENCE PRIOR TO SHELTERED HARBOR

The greatest challenge is generally the smaller industries, they don't believe that enterprise solutions are within their grasp. Whilst BCP is more of a remediation tool for cyber and information security events, when you're a small organization, you think of that as being your data resilience or your ability to recover, BCP and DR seem satisfactory.

Some of the challenges were to get everyone to understand that data recovery, data resilience, and the ability to continue to provide services isn't how long am I going to be offline? It's what can I do to make sure I never go offline? Or if I do go offline, I minimize the impact of being offline.

It just takes a little bit of a different mindset to understand that everyone can be data resilient. Everyone can have multiple pathways to being back online rather than accepting the fact that 8 or 16 or 24 hours offline is what your acceptable risk is.

GETTING EXECUTIVE LEVEL BUY-IN AND PRIORITIZATION

It's really the smaller organizations that think BCP is resilient, but when Sheltered Harbor came on board, with the same philosophy I had been advocating, we were able to change the whole mindset of the bank to go from BCP to data resilience instead.

The biggest turning point, if you want to call it that, was the fact that when you hear enterprise, you think expensive. When you realize that it's not expensive and that enterprise doesn't always mean huge cost, that you probably have resilience built into your BCP program already, you're just not identifying and prioritizing it as resilience.

Once people started realizing that there were a lot of things already in place and that it was just a matter of organizing them, prioritizing them, and documenting them, they started to see the vision come to fruition without having to see huge checks being written.

Data resilience is just a coordination of all the things you're already doing, but putting it in a way that allows you to be back in business faster and not accepting the 8 or 12 or 16 or 72 hour time limit just because somebody wrote that on a piece of paper.

THE IMPLEMENTATION PROCESS & HIGHLIGHTS

FIS are the ones we had initially spoken to about Sheltered Harbor, we followed up and thought it was a really good idea. We liked what we saw. We liked what we heard and we joined.

The initial process to become certified was really easy with FIS as a partner, because they had already built out this infrastructure and the process and they were certified, so we weren't going from scratch as far as the business side of it goes. So the partnership with the banking solution was relatively simple because we were working with a partner that already had a great understanding, they'd already been through the process.

But as we started allowing that framework to bleed into other areas of the bank and our ideas of how we would utilize this same framework for other areas, it became a collaboration, allowing the conversation to be brought up at the same time as cyber security and as information security.

So it was easy to transition because once we developed the process and implemented the framework utilizing FIS, then we started seeing all these dominoes fall and everyone realizes that there isn't a lot of cost to it. We're just moving vertically across the different business units. As it started being put into people's minds, they started making adjustments without really a lot of intervention at all. The key is taking the first step. Once you get it started, it'll just grow.

GETTING OUTSIDE HELP

FIS has been a really good teammate. The managed security personnel at FIS have been very helpful in maintaining a good relationship. I think it would probably be a lot more challenging if they didn't have a partner that was a believer as well in the resilience component.

There wasn't really a need for any kind of other third party. We just allowed it to happen and people inherently started changing their documentation, changing their policies and procedures to incorporate these new philosophies and ideas that all spurred from what we developed and what we were able to gain from having the work group conversations with Sheltered Harbor. So it really didn't require a lot of uplift or bringing in consultants or anything like that.

TECHNOLOGICAL CONSIDERATIONS & CHALLENGES

The biggest key is that you have to have the mindset. The first thing I would advise people to do is learn the difference between data resilience and data recovery. And once you really understand the difference between the two and what the overlaps are between the two, then you are able to start asking questions.

When you go through your business impact, like when we do our analysis so that we can get RTOs and our MTAs and different things like that for our risk assessments, then you start asking why? Why can you last 72 hours? Why is 72 hours your MTA? Why can't it be something else?

WHY SHELTERED HARBOR CERTIFICATION IS IMPORTANT AND HOW IT'S MADE A DIFFERENCE TO YOUR ORGANIZATION?

I think some of the key areas that have started to benefit, is that we're able to pay better attention to actual incident response and dedicate more time to the investigation, the mitigation and that type of analysis rather than everybody worrying about what you're going to do if an incident occurs. So it really bleeds over into all the areas. Most people think about disaster recovery as being a natural disaster or power outage or anything like that, but it's much greater than that.

And when you start looking at it from a data resilience perspective, it doesn't become as unsettling because you have a plan that just needs to be activated. And now you can spend more time and energy on the parts of the business that you can control, which is how do you handle the incident? How do you respond to the types of things that are happening? It gives you more time for, let's say, the SEC and their regulations or CISA and their regulations as far as reporting.

When you have a data resilience plan put in place on top of your DR, it gives you time to actually do those things that are important, whether it be information sharing, whether it be for regulatory concerns, you're able to focus more into those areas because you've done all the other things first.

And you can see those timelines that people are putting on top of you as being reachable and attainable, whereas before the greatest pushback on being able to meet these regulatory timelines was the fact that you're elbow deep into trying to figure it out. I'm trying to recover.

CONCLUSION

I think that the summary of everything that I've learned is: Ask questions. Who, what, where, why, and when. In everything that you do. And once you ask the questions, then listen to the answers. I think that's really the greatest part of what Sheltered Harbor does, is that it helps you understand what questions you should ask. And then it gives you the ability to understand the answers and put them into action. That's how I'd like to sum it up.