SOUTH CENTRAL CONNECTICUT REGIONAL WATER AUTHORITY

AUDIT-RISK COMMITTEE

MAY 25, 2023

MEETING TRANSCRIPTION

[AUDIT-RISK COMMITTEE MEETING BEGINS AT 12:31 P.M.]

David:

Thank you. With that, it's all yours, Catherine.

Catherine:

Great. Okay. First item on the agenda are the approval of the minutes.

David:

So moved.

Catherine:

All right. Moved and seconded. Any discussion? All right. I think everybody's ready to vote. All in favor say, "Aye."

Participants:

Aye.

Catherine:

So that's unanimous. Let's move onto the risk management update.

Rochelle:

I can do some highlights.

Catherine:

Thank you.

Rochelle:

Thanks.

Catherine:

Read my mind.

Rochelle:

We're not going to go through the whole memo, but just a couple highlights before we get into the discussion questions. So, we wanted to highlight that for fiscal 23, the risk management team identified eight additional risks and the goal was five. So, we think that's a positive thing and it represents the evolving nature of what we're doing. And then also for fiscal 2024, the focus will be on a continued risk mitigation review of the risk registers with the idea for redundancy and resiliency.

So, if there's no additional questions on the memo, we can go to the questions.

Catherine:

Sure. There were questions on the end of the memo, so I'd like to discuss them. But one thing that we talked about earlier this week, I think it's worth chatting with the board about... Cybersecurity is a big issue. And right now, there is a great deal of phishing that's going on. I understand that the RWA has been doing some training. Like to hear more about that.

I am personally very concerned that the phishing activity is going to increase and be more dangerous because of AI. And right now, a lot of the phishing is easy to see because there're misspellings and there are other things that pop up. But as artificial intelligence becomes more prevalent and it's used more, it'll be harder and harder to detect that phishing. So, training and making sure that people are very careful about what they open regardless of whether it seemed like it came from Larry, but that makes sure it was Larry and always look at those addresses that [inaudible 00:05:52] things come in. I know that the RWA has been doing some phishing exercises, so it's worth talking about.

You want to talk about what we've done?

Rochelle:

So, for this year... And Prem can also chime in. We've done four phishing exercises. And although it hasn't been 100%, it's been very good as far as the people knowing not to click on the document as well as there is other. We work with Homeland Security. We work with other agencies, and I will share if this is actually breaking news, even in the SNP report, the draft report on our ratings. Actually, they cited how well they think we're doing relative to cyber security, so that was positive-

Catherine:

And also, as we discussed earlier this week, there was no increase in the premium for cyber insurance, right? You have to go somewhere-

Prem:

Maybe if we can add a little bit more color to what Rochelle was saying. To the four phishing campaigns that we have done all the way from... Again, we decided to do four by every quarter and then subsequent training for... Let's say somebody clicked on something they shouldn't, right? So, we made improvements. So, the idea was that 100% of the folks who needs to be involved in terms of their exercise, so we made sure that that person is different than people who actually click on something and then go through a training exercise. So, initially for the first one, we had seven people who clicked on it. For example, for the oral campaign, it has gotten better over the period of the next three exercises we did. The last one we did, we had three people click on the phishing exercise we did. And it was a realistic one because the way we did the last one was asked if somebody internally had sent out this memo, if you will, from a help desk kind of a scenario.

So, people tend to fall for the trap. So, we did a good job on having that training completed. So, I think overall, I think like Rochelle suggest, SNP had quoted many numerous initiatives that we did this year from a phishing standpoint.

AI, Catherine, you mentioned AI, right? That's the big buzzword now. Everybody is talking about AI. So, one of the key things that we did was we have actually I would say blocked AI from a perspective of RWA's network just to be cautious about how our employees are reaching out on this AI platform because there are many examples that were cited in my professional networking as well. The most recent one was Samsung where some of the trade secrets were out because some employees thought it's a good idea for AI to give a presentation of some sat.

So, that was a good example. As soon as we were cited off some of these examples, Tony Perugini, our technology director, along with Kevin Schnaittman, we had put some controls in place where we don't have direct access for employees to go on to some kind of AI platform, provided if there's a business reason, we have made probably one or two exceptions where it's under full control in terms of how our employees access AI. So, those are some of the things we put in place.

And more recently, there was actually Homeland Security is what they call as ransomware readiness assessment. We actually went through the ransomware readiness assessment, and we came back with flying colors. So, in terms of what Homeland Security has found recommendations, there are literally no recommendations from our perspective because we are fully in compliance.

The second one that happened more recently was EPA. They actually had what they call is WCAT which is Water Cyber Assessment Toolkit. So, they actually launched that and then, they actually asked water companies to go ahead and do the assessment. So, again, we completed the assessment in regulation with what EPA had put out. And we didn't really have any of the threats as we would not including AI, right? We have those controls in place.

So, I just wanted to add this color to get more awareness and education if you will. Also, we are constantly looking at it. We do have a cyber, I would call capital plan, a five-year plan that we have. We constantly assist that. For example, next year, we have a couple of things such as security operations center. We are trying to create a formal tool set if you will.

Again, going back to working with Homeland Security. So, we are trying to put those measures in place to really kind of strengthen and bolster our cyber posture. I'll take it faster. There's a lot more to cover, right? But just to get a good feel in terms of our phishing exercise and what we are putting in play and some of the assessment, I think we've been doing a fabulous job.

Catherine:

I would agree.

David:

I don't know if comfortable is the right word because you never should be comfortable, but I'm satisfied that the Authority does a great job in that aspect of it. I'd like to know a little bit more about the other side of it, and that is if we did get an attack, are we prepared? Do we know what to do if somehow SCADA was frozen, somebody got into it? We couldn't adjust the water levels, and the chemical levels and all that. Have we had any exercises on that? Because I know between Kevin's committee, we've talked about having a lot of tabletop exercise. I don't know if it's-

Amanda:

That's right. Can I chime in here a little bit to clarify some of that as well, Larry and Dave?

David:

Yes.

Amanda:

Okay. That's a great question. So, we actually did a BCP exercise for SAP system, this is many months ago, in terms of a breach that could happen on our data for example. So, the team actually did a full-blown exercise on that. If you remember we did an exercise, we picked a smaller treatment plan and then, we actually exercise manual operations for event of getting compromised on the SCADA system. So, we did those two exercise. We do have one coming up. We are planning in the next fiscal year. This is for Cheshire water treatment plant, so we are looking at doing a bigger scale exercise to really figure out if you're really ready from our pump station operations.

So, we have been from time to time doing some of these exercises, David. And like you said, this is one thing that keeps me up at night, so I'm constantly looking at some of these things. And last week, as an example, we had a situation where we call it as [inaudible 00:12:50]. Attacker is going out in the web from Pakistan, so Kevin Schnaittman was looking at it. While we are not vulnerable, we were made aware of the situation, and we closely tied back with FBI.

So, those things are in play. And to your point... Or one thing we'll definitely do much more. I know last one, Catherine, was part of this exercise for the manual operations. We will do more of that and make sure that the board is more involved, so you feel more comfortable from a BCP standpoint. So, hope that's helpful.

David:

Thank you.

Rochelle:

Can I also just add? We do have under our insurance, and hopefully it won't happen, but we actually can call and even... Because we also had a BCP on actually ransom and whether or not, we would pay it or not and how we do have access to a professional team to help us through.

David:

But I assume that part but [inaudible 00:13:45]. Thank you. That's very interesting.

Sunny:

Just to add to what Prem said on that BCP exercise. We even went to the extent of supply chain issues where Alan Bradley PLC was not going to be available within 24 hours or 48 hours. So, we simulated to see whether we can actually take that kind of a tolerance. So, we were able to do it and went into manual operations and saw how it works.

So, the BCP exercises are well-thought-out. There is teams from all over, I would say across the entire, I would say all domains come in. They provide the inputs, and we develop the program. And sometimes the participants are not kept aware. So, in that way, all the participants are really, I would say you

simulate the condition as if it's happening. So, it was a very, I would say, elaborate exercise that happened on that pump station.

Prem:

So, I think if I may suggest something, right? Again, going back to the time that we have in terms of boards allocation, et cetera, we have Kate Novick who really does a very good job on the BCP. So, we could pull up some of the things as examples we did and share with the board to feel more comfortable, and for any suggestions that you may have, so we can do that as well as a follow-up item.

Catherine:

Thanks, Prem. There are some questions at the end about what our risk tolerance is. I don't have any tolerance.

David:

I agree.

Catherine:

Yes. And I think it's worth identifying that these risks are all interrelated. Cyber risk can affect water quality, and the challenges that we have in protecting the property around our reservoir or reserve can also be theoretically. It could have that water quality as well. All of these things are interrelated, and I think it's important that we keep an eye on all stuff.

David:

And then, we continue as a board, get the oversight reports and know that we're doing our job well.

Catherine:

Yes. Exactly. Are there any other questions?

Rochelle:

No, the only other thing I would say is that, for the last 20 years in the financial services industry, which has gone through a lot in 2008, the world melted down because there was a whole bunch of risks that wasn't being assessed properly. And I think that lessons learned from there were really about doing the walkthroughs on the worst case scenario that anybody could conceive of and the follow through of what you do afterwards. And it was even scenarios that's like, "Well, that'll never happen." Well, guess what, right? I think we keep doing that and the worst case scenarios of what do we do when that happens. I think we're in good shape, but I think we need to make sure we're comforted that the worst case scenarios aren't-

David:

Aren't addressed.

Rochelle:

Yes.

Catherine:

Kevin, did you have anything?

Kevin:

No, thank you. I thought it was informative.

Catherine:

We can move on to the work plan for 2024. It's actually pretty similar to 2023. Are there any questions, concerns, or changes? The only change of [inaudible 00:17:39] what we're doing in December.

Rochelle:

So, we have two internal audits. Well, one definite and another possible. We talked about back in December 2022 engaging a third party. So, we're moving forward with doing that and we're proposing. It's up to the committee to do the fraud control and the knowledge transfer for fiscal 2024 audits.

Larry:

That was when we asked Congress need to come in and do an assessment of our internal audit. They identified those two areas that they recommended be the first one to pursue as part of an internal audit. And the certain-

Catherine:

Can you say the two areas again?

Rochelle:

Broad control and knowledge transfer.

David:

Knowledge transfer. Okay.

Catherine:

What is knowledge transfer?

Rochelle:

Knowledge transfer. This is the risk... Yes. Everything associated, documenting our processes and assumption-

Larry:

Both the formal and informal ways, being able to pass down that knowledge that nobody else knows how to do in an organization like putting that valve over sort of thing and nobody know that.

Catherine:

Okay. Thank you.

David:

I'm much more [inaudible 00:18:51].

Catherine:

All right. But it's not something we approve but any either questions. In that case, I entertain a motion to adjourn.

David:

I move we adjourn as the Audit Risk committee and meet as the Environmental, Health &

Safety Committee.

Suzanne:

I second.

Catherine:

All in favor?

Committee:

Aye.

[AUDIT-RISK COMMITTEE ENDS AT 12:47 P.M.]