SOUTH CENTRAL CONNECTICUT REGIONAL WATER AUTHORITY

AUDIT-RISK COMMITTEE

DECEMBER 15, 2022

MEETING TRANSCRIPTION

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

Catherine:

Okay. Good afternoon everybody. First item on the agenda, entertain a motion to approve the minutes from the September 22nd meeting of the Audit-Risk Committee.

Tony:

So moved.

Suzanne:

And I'll second Catherine.

Catherine:

It's been moved and seconded to approve the minutes of the September 22nd meeting. Is there any discussion? Hearing none. I'll call for the vote. All in favor, signify by saying aye.

Attendees:

Aye.

Catherine:

Any nays? No abstentions. Motion carries. Next item on our agenda is a discussion of the controls and risk assessment update memorandum. This is a matter that involves security strategies and the implementation thereof, and I would entertain a motion to go into executive session.

Tony:

So moved

Suzanne:

And I'll second that motion.

Catherine:

Okay. It's been moved and seconded to go into executive session to discuss matters that are exempt from disclosure pursuant to Connecticut General Statute 1-2006C. All in favor signify by saying aye.

Attendees:

Aye.

Catherine:

Looks like it was unanimous. So we are now in executive session.

Jennifer:

Catherine. I'm sorry, Kevin Schnaitmann is here. Is he supposed to be here for executive session Prem or is he supposed to come after?

Prem:

Not yet. He would come afterward.

Prem:

Okay. Kevin, if you don't mind, I'll text you.

Catherine:

Well, we need to also identify those individuals that were inviting into executive session? Larry?

Larry:

Yes. I would like to invite the leadership team, and my staff that report to me, as well as the executive board administrator.

David:

Thank you.

[EXECUTIVE SESSION FROM 12:32 P.M. TO 12:44 P.M.]

Catherine:

Forward to Prem.

Prem:

Thank you. Catherine, if you don't mind to pull up the two page memo, Jennifer. Thank you. So I'm going to keep it at a very high level. There is a reason why we did not put a lot of details because it's not in the executive session here. So if you have any questions, of course, please stop me. So for this second quarter update, what we did was we focused on specifically five different areas that we wanted to provide an update on. As you had look through the memo, it's pretty straightforward. For the fiscal year '23 for the top three cybersecurity areas, we have been focusing quite a bit on things that actually had come forward as either a requirement or a compliance for example, whether it's DHS or CISA or Beazley for example. So the three focus areas at a very highest level that we kept was multifactor authentication.

I'm sure you probably heard about MFAs or multifactor authentication. We had put that in place for both our business and scale network, which is a big, I would say even a requirement for our Beazley insurance. So we took care of that. And then we also had been sent some additional requirements, a supplemental as they call it for Beazley's ransomware audit. The team had filled all of that question and I think from perspective of having continuity on the insurance, this is pretty critical. We'll be submitting that specific details back to Beazley in March. So the team is putting through that. We do have insurance today, so I'm very confident and positive about continuing to have the insurance coverage for us. Just as a point of reference, as I talk to our peers in industry, et cetera, we have been hearing about 50 to 60% of dropout on the insurance coverage for different companies. That's a pretty huge number. It's just increasing.

So that makes us feel even more comfortable and confident that we are able to continue to implement the requirements as they come up. MFA was just one of them. So the last one in this section was really along the lines of being more proactive as we work pretty closely with FBI and DHS. But I think we went one beyond where we tried to practically report back to them in terms of, for attacks and other things that happens in a more proactive fashion. So that had been pretty very well received and need to strengthen the relationship with our external parties there. The second one, sorry Jennifer, we go up a little bit.

The second one was the cyber update. Very high level fiscal '23 related items. We pretty much have already implemented and put in place. So we've been doing pretty good on the roadmap. We do have identified three different items for next fiscal year. Very high level on that, additional scans for scale system was one of them. We are looking at doing an insider set awareness program for our employees. This is another requirement which we think is going to come pretty soon from our insurance carriers. So we are looking at that for fiscal '24. So we are working with corporate services to really put that in play for all our employees. The last but not least in that section is really strengthening our ATNT network for resiliency purposes. That's part of our roadmap as well for fiscal '24. So as you all aware, these threats are real and these happen, pretty new threats we see almost every other day. So we are trying to keep up.

So we do update our roadmap on a quarterly basis, so we are pretty close. Typically, other companies do it on a yearly basis, but we are even more aggressive and proactive about that. So that's a little bit of second section there. The third piece of that update was also the Fountain Lake exercise. I'm sure some of our authority members here participated along with our RPB members. It was a very good exercise. We did it on October 21st, approximately around 30 people participated internal and external team. Overall, the exercise was pretty successful. This is really to look at our worst case scenario. If you remember, for whatever reasons, if our cyber network is compromised, can we switch back to manual operations? That's in a sense what we try to demonstrate there. Typically, again, this is a good one because it also talks about how ready we are in terms of preparing ourselves.

So that was a good exercise and then we did have some lessons learned that came about it. One of them was being able to prioritize upon stations. We do have a change in staff as you know, we just want to make sure we are keeping them as the knowledge owners and being able to demonstrate whenever it's needed. Some of the past deals, as you know, our subject matter expert, the team does a great job. They come together pretty well, things of the sort. So more to come. We are planning for a bigger exercise just for the team here. So next fiscal year, we are looking at most likely at the Lake [inaudible 00:05:29] pump station. We'll have onsite presence et cetera. So it is a much more robust exercise. So we'll be doing that next fiscal year. So that's already under works in terms of planning.

The fourth one we wanted to talk a little bit about was the Phishing Campaign. Again, this is one of our global metrics as you're aware. We did launch two of them for the past two quarters. We have done pretty well. We have a 99% success rate. That's really good. The first one had just one employee fall off. The second one had three employees fall off. I won't go to the employees. So it is a good one. I think we are very, very confident and comfortable in terms of where we are. We also have launched a real-time training right after, for example, the three employees fallout. We just help them to see what they clicked, what they were supposed to be doing. So it was really, very well received and again this is one of the ideas of being more proactive. So that's the good news there. The next two are planned for future, like in January, this one and then this April is another one. So that should be one of our global metrics accomplishment.

The last but not least, in terms of the update is the CISA dashboard. We did a very good job in our penetration test as you know, we actively tried to take the help from the DHS. There were no known vulnerabilities at this point. We have a full-fledged dashboard. Again, for security purposes, it's not here and we can provide a copy in any of our authority members who would like to see it. So the top three things we look at in terms of that specific dashboard is, do we have unsupported software? Do we have any potential risk to our open services that can receive through the internet? So all of those things were being tested with the penetration test. Again, we do a weekly test. So again, it's very intensive. So far, so good.

Those were some of the big updates for the second quarter. We did wanted to see if the authority had questions and as you're hearing through some of these updates, how confident does the board feel? Any questions for us along those lines? Again, I know there was a little bit of that pre-pandemic people working from home. We got a lot more VPN scenario where people are logging in, our employees. So we want to really put the question as, is there anything that board really wants us to cover as a topic or does the board feel that we are doing enough? So again, this is for the topic of discussion here.

Catherine:

Well the one thing I did want to point out, 99% is a great score on a math test, but with respect to phishing and other vulnerabilities, it only takes one time in order to get into our system. And we went from one error in August to three in November. 99% gives me a high level of comfort. It's that 1% that always is of concern. And so I don't think that you should call out employees, but I definitely think you should let people know that, it only takes the one time.

Prem:

Absolutely. Yeah, Catherine, right. And I think one of the things that we try to do here in terms of the Phishing Campaign, we get more creative, we make it more real. So for instance, the second one was to make them feel that an employee called them and there's a voicemail. So we make it real. The next one is going to be as the leadership team members sending an email. So we are trying to feel,, to see how the employees are prepared in their mind. But you're absolutely right that one click is all that is needed to get us compromised and that's where we are trying to train them.

So this phishing campaign is a great avenue to train. Again while we talk about different protections like firewalls and the different networks. So we do have those protection in place. But I agree with you when I think we will continue this creative way of phishing. And again, another point of reference I could say is that when you look at outside with other companies, I'm just comparing to our peers, [inaudible 00:10:06] in other places that we have as our neighbors, their campaign rates are at 80%. So when I think about that, I feel much more comfortable. But I agree with you, that one click is all that matters and we need to strive for that.

Catherine:

I always remember when you're being chased by a lion, you only have to run faster than the slowest person.

Prem:

That's funny.

Tony:

I resent that.

Kevin:

Yeah. I also want to mention that yes, you're only as strong as your weakest user when it comes to email. But we have a much more layered approach so that if that does get clicked, we do have antivirus, we do have malware, we do have greyware, we do have web filtering that blocks known spam sites. So there's a whole bunch of other protections and just to even get some of these emails through, requires me to allow a lot of things to happen for that click to happen in these emails.

So it's a multi-layer approach knowing that and we have to assume that yes, a user could click on it by accident or a user could do something that they're not supposed to do. One level is to train the users, but it's also just to make sure that our backend protection is also as strong as knowing a user may click on something. So there are a lot of other protections in place if an email does get through or if a user does click on links, that there are some other systems in place that would most likely prevent that from downloading that malware or that Trojan into our network.

Catherine:

Thank you, Kevin. That's great to hear.

Prem:

Yep.

Catherine:

I had one more question but I wanted to see whether there were other members that had questions, comments.

David:

I do have a question, it's question and a comment if I could, Catherine. In item one, we write that DHS does the weekly testing and all, but Tony may recall that when we started doing this, we weren't all that sure that they had the experience to do the super job that we needed to be done it almost a joke, don't give the government something to do that you really have to have done right. Do we have a backup to somebody else doing this on a somewhat regular basis as well or are we relying simply on this one source to be our testing?

Kevin:

I'll cover that Prem. So Department of Homeland Security is using one of the best tools in the industry to do these scans. It's one of the same tools that we use internally for our own internal vulnerability scanning. So the product they use is Nessus and it's a known security tool. What they do is they have an automated scanning of all of our live IP addresses in the external world or as far as internet facing and they scan that weekly and they provide us a report from that. We have the ability to also do our own scans using the same tool that they're using to scan our external addresses. And we do that randomly. It's not so much probably on a quarterly basis, we'll take a look at some things, especially if we ever change any of our external firewall rules. We will scan for vulnerabilities before waiting for Department of Homeland Security to discover anything. We also use our tools inside. Anytime we add a new piece of hardware, a new printer, a new switch, we will do a vulnerability scan on that before we put it onto the network.

Prem:

Yeah. I think I also wanted to add a couple things David. So I've seen a multitude of other products like Phantom. There are many products out there, but fundamentally, they build off of what we have from CISA, right? The Nessus tool is the base for some of that. And then there's also, from a coverage standpoint too. So when a question arises, if for whatever reason you get hit, they will be running through the same tool. So they will ask, that's the first question, "Did you do that, right?" I think from that perspective too, it's pretty good.

So I believe that from cover standpoint, like Kevin mentioned we got different layers of protection and then on top of it, we have this weekly scan. And then I also feel like to some degree, these proactive measures we are taking where we are informing them to be able to make better of the tool that we have, it is actually a big deal right there. So I feel confident, but again, as you know, we only know what we know and then I think yesterday or day before there was a whole Cuba ransomware situation. I know Kevin texted and he was just talking about... So there are things that keep rising and we adjust based on what we see, much more in a robust way and it's not more a reactive way. So I think that all helps us to stay protected if you will.

Kevin:

And they have found vulnerabilities in the past. So it has been a good service. So remember, I think it was last year around this time we were talking about the LOG4J vulnerability and we did have a device out there that had the LOG4J vulnerability at some time and we were able to shut that down and prevent it from being on the internet. So there's service, even though it comes back as being clean most of the time, it's good to know that they're there scanning it and we do see them scanning it, so it's not so much do we know that they're doing it. We absolutely know they're doing it. They trigger logs every Friday and Saturday. So IT department and myself will get a ton of logs, email alerts that somebody's doing something they're not supposed to be doing, scanning our network. So we're able to see that it's them that they're performing that. And then they do send us a report on Mondays after their weekly scan. So we do know that they're actively doing it and the tool that they're using is a tool that we're familiar with as well.

David:

Great, thank you very much. Appreciate it gentlemen.

Catherine:

Thanks. Are there any other questions or comments on this section? Okay. Prem, I just have one quick question. I too am aware that there are a number of companies that are finding themselves in a position where they cannot get cyber insurance coverage because they're not meeting the minimum requirements. I'm glad to hear that looks like we're heading in the direction of a renewal. Are you anticipating a significant increase in cost?

Prem:

I'm thinking again, if I say no, Amanda will slap my hand. So I do expect a 50% increase. But that being said, I think for all the right reasons and I don't want to mention about the coverage here, and it's a public session. We have also increased our coverage requirement as well. So I do think it's going to be a little bit, I would say 40, 50% over, but it would also get extra coverage. And I do have the questionnaire with me, Catherine. I know you'd asked if I can share. So I do have the questionnaire. Kevin sent it to me so I'll send it to you. So the one that they sent for supplemental and then what we had answered. When I look at all those different answers, I'm very confident that we will get the coverage. So it has to go through underwriting, I believe it's March, April timeline. So we will go through that exercise but I'm confident that we'll be fine.

Kevin:

We have also this year, Prem and everyone, we had added as one of our risk perspectives for the risk committee that we've added a risk to cover, see if we had to self-insure so that we've added a new risk perspective this year related to cyber insurance. So we're taking that very seriously because there is a chance that the insurance companies may not provide that anymore due to the risk out there. So we've added that as one of our new risk perspectives that'll be submitted, I believe February timeframe as it relates to ransomware insurance.

Catherine:

Thank you. Unless there are other questions, I think that we will adjourn as the Audit-Risk Committee.

David:

So moved.

Prem:

Thank you everyone.

Tony:

Second.

Catherine:

All right. It's been moved and seconded. All in favor?

Attendees:

Aye.

Catherine:

All right. I heard four, so that's unanimous. And we are moving on. I give it back to you, Mr. Chairman.

[AUDIT-RISK COMMITTEE MEETING ENDS AT 1:03 P.M.]