Lowenstein Sandler's Cybersecurity Awareness Series

Session 2-
How to Prepare for a Cybersecurity Breach

By Kathleen McGee and Ken Fishkin
OCTOBER 2021

Ken Fishkin: Hi, welcome to Lowenstein Sandler's Cybersecurity Series. And today we're going to talk about how to prepare for a breach.

Kathleen McGee: In fact, Ken, we're going to be talking about something really specific called running a tabletop exercise. Maybe we could start by you telling us what a tabletop exercise is.

Ken Fishkin: Well, Kathleen, it's really more like a fire drill or a dry run in case you do have something like ransomware or some other kind of data breach impacting your organization. This way, you have all the players at the table. And that could be like the head of HR, head of marketing, operations, IT, security– get them all in one place and run through scenarios, so that way, they are all feeling good about a particular situation should it happen.

Kathleen McGee: Great. Let's break it down for our, for our viewers today. Who's coming to the tabletop, and does it actually have to be around a table?

Ken Fishkin: So in the old days, two years ago, it was around the table. But now it could be done on Zoom, and it really doesn't matter as long as everybody is in, you know, can hear each other and you have good communication. That's really the point of this tabletop exercise is that everybody can discuss weaknesses within their plan, or if they're just starting a new plan, flesh out all the, all the different ideas they have and get everything on the table, so to speak. And that's really where it's going. And you really should have the head of every department that would be potentially impacted by that ransomware.

Kathleen McGee: Got it. One thing that I've learned with our clients over the years is it's also always important that that one key person also has a backup, because amazingly, people sometimes go on vacation. So I know in another session we had talked to our viewers about pulling together the basics on a cybersecurity plan. I've found that the tabletop also really helps you test that plan and find out where there might be holes that you can then build on.

Ken Fishkin: Yeah, and that's really the whole purpose of a tabletop exercise, is to go through it and see where you need improvements, because every time you do things ... I mean, you should redo it every year, really, because things change over time. You know, for example, ransomware was just ... it used to be that they would hold your data, you know, make it unusable if you didn't pay, but today, they're making it public, so that's a new concern that you

wouldn't have thought about two years ago. So it's important to be current and continue these tabletop exercises.

Kathleen McGee: I agree. So, who is running the tabletop?

Ken Fishkin: So the person that should be or the team that should be running that tabletop exercise is really somebody usually outside of your organization, or if they have great knowledge, if that's their job, is to stay on top of that, you could be, ah, done internally, but you really want somebody who has that expertise of what could happen, who has that experience of what happens during a breach and is staying on top of the laws and staying in touch with police enforcement, law enforcement, and really understands it from all different aspects.

Kathleen McGee: When you're doing a tabletop exercise, you said you're considering all the various scenarios. I think you were going to walk us through some details of a specific scenario, and I'm pretty sure it was ransomware.

Ken Fishkin: Yeah, ransomware is the king of cyberattacks right now, especially since Colonial Pipeline, everybody's familiar with what could, what could happen to infrastructure now. So, and now you just bring it down to your own organization, if your whole organization was crippled by something like this, where all your machines were down. Imagine coming into a building one day and the sign said go back home because all systems are down. I mean, that is what happens with ransomware. And it's very scary. So when you're doing a tabletop exercise, you want to start out by going through those motions; you can take it in baby steps, so you could say that one machine is infected by ransomware. What does the organization need to do? Do you just need to wipe that machine? What if that machine had sensitive information on it? What if you find out that that machine has also impacted other machines, and one of them is your client database? So you have no idea what the scope of that breach could be. And you have to ... you have to be really, you have to be familiar with that kind of incident in order to prepare for that.

Kathleen McGee: I think the other thing that I've found over the years with clients is the more you run these tabletop exercises, the more it becomes muscle memory, which is precisely what you need when you only have 48 hours to respond. You don't want there to suddenly be an incident and no one remembers what it is that they're supposed to do. So the more often you run these, the more likely it is that someone's just going to automatically respond the way you intended.

Ken Fishkin: Yeah, absolutely. I mean, like these ransomware attacks, they only give you a certain amount of time to make a decision. And it's really key to have what I call a playbook, and/or an incident response policy, where it really details the roles and responsibilities that everybody has and walks you through what needs to be done in every level, in every step, during the investigation, while you're trying to identify what the issue is, all the way to dealing with public relations and dealing with potentially giving credit-monitoring services to your customers.

Kathleen McGee: Who, in your experience, authors or helps to author that playbook?

Ken Fishkin: Yeah, so that's where legal counsel really comes in. They are excellent at making sure that you dot your ... dot your i's and cross your t's as far as making sure that you understand all the legal ramifications that could happen during this type of incident, especially when you're dealing with privileged information.

Kathleen McGee: Absolutely. And that's a big thing that I know I've hammered on other sessions that we've talked about with our audience here, the importance of understanding how to message what is happening in a way that is just compliant with the facts as well as regulations; you may also have third-party contracts that are requiring certain types of disclosures, and it doesn't matter who your communication is geared to– everyone's going to be reading it. So it's really important that you craft your communications and take a look at the facts that you have with a lawyer in place. And it does certainly help to draft that playbook with, with your lawyer at the very start. The other thing that I think is important–and I know, again, we've talked about this in another session–but making sure that you, that you have a plan for identifying your cyber insurance company, because at this point in the game, we know everyone has cyber insurance where they should, and we've talked about that before as well. The communications, and I think perhaps one of the most important things, contacting law enforcement–I found that can be a really controversial concept for people, and it's important to play out in a tabletop exercise first.

Ken Fishkin: Yeah, absolutely. We bring law enforcement in for every, every time we run one of these exercises. They may not be exactly at the table when we're doing it, but they make sure that we are thinking what the latest scams are and what's going on as far as in, in their world.

Kathleen McGee: So if you go on to the FBI's website, any one of our viewers can find the contact information for their local field office. And in fact, if you reach out to them and let them know that you're working on developing a tabletop exercise, they can help provide you information. They may even be able to provide you with contact information for someone who can do a site visit, who can attend your tabletop, or who can at least provide some guidance. And I think, most importantly, you then have a number to call if a real incident happens.

Ken Fishkin: Yeah, you should absolutely contact law enforcement even if you think the incident might be minor, because they will respond and act appropriately depending ... regardless of the severity of the issue.

Kathleen McGee: We have found as well, and that was also really highly publicized in the pipeline incident, but even in smaller cases that our clients are dealing with, sometimes the FBI actually has information on decryption keys to help get you back that information. Sometimes–not often, but sometimes–can help you recover some of the ransomware that you might've paid, but certainly to help pay that forward and help the next company that's maybe going to fall victim to a ransomware attack. I agree, it never hurts and it could help to call

law enforcement, and so it should always be part of the tabletop exercise. But again, it's really important that you are open and have that conversation as an organization before an incident happens, and that's one of the reasons why tabletops are so important.

Ken Fishkin: I agree.

Kathleen McGee: Well, I feel like we've run through some of the basics for a tabletop exercise, and hopefully it gives some people some food for thought about how to plan for their next one or maybe get started on one in the first place. Thanks so much, Ken.

Ken Fishkin: Thank you, Kathleen.