Lowenstein Sandler's Cybersecurity Awareness Series

Session 1 -
How to Protect your Organization From a Cybersecurity Attack

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 protect your organization from a potential attack. We're going to talk about what happens if you do get attacked during a breach. And we're also going to discuss some of the threats that might happen and how they get into your network. I'm Ken Fishkin, and I am the, in charge of the information security and privacy for Lowenstein Sandler.

Kathleen McGee: Hi, Ken. I'm Kathleen McGee. I'm a partner with Lowenstein Sandler's tech group as well as the white collar criminal defense group. So in this session, we are going to be discussing what I like to call an ounce of prevention is worth a pound of cure. And so we're going to be focusing on what an organization can do to lay the groundwork for either creating or enhancing existing cybersecurity systems. I think we have to start with you, Ken, because you have a lot of experience in this. So tell us, what are some of the foundational elements for good cybersecurity? What should people be thinking about when they're evaluating their organization?

Ken Fishkin: Well, the first thing that comes to mind is that you have to protect, you have to understand what assets you have–and by assets, I mean computers, phones, anything that's plugged into a company's network–and you have to make sure that they are patched as well. And that anything that's old and no longer supported by a vendor needs to be replaced or upgraded.

Kathleen McGee: So let me break that down for our viewers today; we're talking about inventory of hardware, everything that gets plugged in. What about for people who are working remotely?

Ken Fishkin: Yeah, so when it comes to that kind of equipment, it's important that if you make a connection to your home base–it's called a virtual private network–that you're using machines that are supported by the vendor. And there's ways that you can check when you go and make that connection to your main office that you have proper antivirus software, that you have an operating system that is supported by the vendor, and you might have some other things or requirements in order to get onto the network as well.

Kathleen McGee: Okay. So an organization should make sure that they have a list of all the possible equipment that could get plugged in so they know what they have and they know maybe how old it is or what it's capable of doing. You spoke also, though, about software a little bit. Can you elaborate for the viewer on that?

Ken Fishkin: Yeah, so a lot of times people don't update their software, and it gets old, and as a result, there are weaknesses within that software–they're called vulnerabilities–and that's what hackers use to get into systems. So like, for example, like Adobe might, if you're using an old version of Adobe that has a known vulnerability, a hacker can go in there and take over a computer just because you have an old version.

Kathleen McGee: So how does an organization know if they need to update software or take care of what you're calling patches?

Ken Fishkin: Yeah. So basically, you have a ... you can install, you can use tools that would, that basically gather that inventory for you and let you know where those holes are and what you need to patch.

Kathleen McGee: So we've talked a bit about hardware. We've talked about software, but are there other tricks of the trade that you would recommend for organizations?

Ken Fishkin: So a lot of times, it's human nature that we have all these passwords that we have to remember for work and for personal use, and what I recommend people do is enable something called two-factor authentication when they're trying to get from their home computers to the office. And what that means is basically–and many of you have seen it before–it's something that you know, like a password, and something that you have, like your phone. So, for example, when you call up a bank and they want to verify that you are who you say you are, they will send a code to your phone, and you will have to read that code back to them. That's two-factor authentication. And I highly recommend that anybody, any company, employ that onto their systems, so that way, the home computer, now you know who that user is, and it's not some hacker coming in from the outside.

Kathleen McGee: And just to clarify, while it's extra recommended for organizations that have people working remotely, I've also certainly seen clients, especially clients who really have sent extra-sensitive information, they use two-factor authentication when anyone logs on to a device, even if it's in an actual office. Have you seen that?

Ken Fishkin: Absolutely. So I mean, banks, for example–that's a, you know, that's a place where it's highly regulated, and they have much more controls than a lot of other organizations might, might, might have. That's definitely a place where you need it. I've seen it where it's pretty cool, where your, your, your token, to ... your access card to get into your building. You can take that card, and you put it into your computer, and then you can use that for two-factor authentication, and it works pretty seamlessly.

Kathleen McGee: Certainly familiar with it, and that can be a bit of a pain, but understand that it's one of those things that we should not be avoiding–it should be a necessary requirement for all staff or just particular staff working in an organization?

Ken Fishkin: It should be for all staff, yes.

Kathleen McGee: That's good to know. We're talking about staff. What about the human element when it comes to working with cybersecurity? What should we be thinking about with our people?

Voice offscreen: Right.

Ken Fishkin: The challenge that somebody in IT always faces is the human element. And it's something that we really can't control too much. And the biggest threat that we've, that we see right now as far as employees, is email, and people click on links, they open up attachments when they respond to emails that are not real. And they're, well, they're real, they're hackers, and they're pretending to be somebody else. And there's all these different scams. So I try my best to educate our employees by sending fake scams about gift cards or about the latest types of attacks that are going on so that way, when a real one does come along, they have a little bit of a heads-up. So, and we always, we always have some tools in place to scan attachments or to verify links, as a backup, because everybody can fall for, you know, a fake email, and myself included, you know, when you're rushing and trying to do something, you know. We're all prone to make mistakes.

Kathleen McGee: We are all prone. I know that we're talking a little bit about training people and educating people. Are we talking about just a certain subset of an organization, or does everybody need to get trained? And having those training mechanisms for your clients that don't upload, don't download, don't click unless you're sure, and those tricks of the trade–it seems to me that's an ongoing education process.

Ken Fishkin: So every company, you know, has a different way of doing this, but I'm a firm believer of always, constantly having training in all different formats. You can have some formal training periodically, and then you can have informal training, like those phishing scams that I pull on my ... with the employees. And you can also just send alerts about this is the latest thing that's going on. So there's all different ways that you can educate people about what's going on, and you can even make games about it, like, you know, give prizes to people who, who, who, who's the first person to get the scam, so you can make it fun as well. So we're trying all different techniques, and it's an ongoing process.

Kathleen McGee: Yes, you are. One last thing that I wanted to ask you about is just an organization understanding where they're holding their data. You had talked about servers before, but also the importance of knowing what information you're actually collecting, what, what it is you're trying to protect. Can you talk to us a little bit about that?

Ken Fishkin: Yeah. A lot of times, companies don't even know where their sensitive information is, so it's very hard to know how to protect something if you don't know exactly what you are protecting. So, like I was saying before, you needed to get an inventory of all your devices, computers; you also need to get an inventory of where your data is and what your ... and, and prioritize it. And that way, you know how to protect it, so if you have some information that's in the cloud, you have to make sure that that's protected as, as, as best

as you can and do a real inventory. And that may include doing interviews with people, because let's say you're with a client and you're doing something that's unusual, but you don't tell IT about it. So IT can't tell you the proper way to protect things if they don't know about it.

Kathleen McGee: That makes sense. We're talking a lot about protecting information. One of the other reasons that we encourage our clients to protect information isn't just because they're worried about their exposure. They also have contractual obligations, right? You have business relationships, or you're worried about government regulations in order to maintain good cybersecurity. And that's where people like me come in–the lawyers. I, you know, I guess one thing that I wanted to focus on for organizations is understanding the role that law and lawyers play in cybersecurity. So I thought I'd run through some of those things for our viewers today.

Ken Fishkin: Yeah, absolutely.

Kathleen McGee: Once you have these procedures in place–you've trained your staff, you've got a handle on what your hardware is, you are working on a program where you know what your software is–you need to think about and highly recommend that people get a cyber insurance policy. You may have basic coverage, you may have D&O coverage on your policies, you may even have business interruption policies with your insurance company, but a cyber insurance policy is going to provide the additional coverage that I think clients need to ensure that when an incident happens–and the likelihood is, unfortunately, something is going to happen–that clients have the opportunity to file a claim and get some coverage. I'm dealing with a ransomware event right now where there was no coverage. I dealt with one two weeks ago where they had great coverage. And I can tell you it's night and day.

Ken Fishkin: Yeah, no, cyber insurance is critical, and there's even some regulations that require cyber insurance to be a part of doing business.

Kathleen McGee: That's right. And you know, certainly I think, more and more, it's impossible to even get a cyber insurance policy unless you have good basic cyber insurance practices in your organization. So if you want to know which comes first, chicken or egg, I can tell you it's the practices that you've been laying out, Ken, but then immediately following that is take a look at your existing cyber insurance policy to see if you can increase coverage, and if you don't have a policy, now's the time to get one. You know, I think the other question that a lot of people ask is “Do I really need to work with a lawyer when it comes to these sorts of things?” And I think, unfortunately, the answer is yes. It's really important to have someone who's an outside counsel, who's going to provide that touchstone on all the various regulations that you've referred to just now as well as ensuring that their insurance policy and other policies are going to be considered reasonable both to their business partners–and there may be contracts that require that now, often they do–but also to regulators, because if there is an incident and you do have to report it, and the likelihood is you probably will, they're going to want to know whether or not you had those reasonable practices that you've been describing.

Ken Fishkin: Yeah, and you also have only a certain amount of time before you have to tell people that you have the breach. Some of them, sometimes it's like 72 hours. It's not that much time.

Kathleen McGee: Yeah.

Ken Fishkin: So if you don't have your ducks in a row, you know, you could be fined.

Kathleen McGee: Right. You could be fined, and it could create additional business friction with your existing business partners and could cause you some real financial losses if you have to think about horrible terms like indemnification–the worst term ever for people. So there are a lot of concerns there as well. Another thing that I really wanted to point out to our listeners is thinking ahead about whether or not you are the type of person that feels comfortable, for example, paying ransom if you have a ransomware event; thinking about establishing a relationship with a PR company or working with your internal people, your internal staff, on communications–who would be the point person for that? And I know we're going to talk more about that in our ... in another session that we're doing, which is called the running the tabletop; it'll be really exciting, what to do in those fire drills.

Kathleen McGee: But you know, often I help our clients prepare by talking to them about who goes where and why when it comes to communications and dealing with regulators; those things go hand in glove. Again, you'd never want to say anything that's going to potentially increase your exposure unnecessarily. Always want to be truthful, but you want to own, you don't want to get out beyond your skis when it comes to communications. But you also want to make sure that while you're doing the work of unfortunately dealing with a cleanup if you have to, that the communications are as privileged as possible so that you can focus on fixing the problem and not have to worry about the lawsuit that may or may not come out of that. And that is one of the big reasons why people include outside counsel like yours truly so that they can help to navigate and manage protecting for privilege.

Ken Fishkin: Yeah, and I agree completely. And anything you can do in advance, like even making a template of what your response would be for a breach ahead of time would be of great value.

Kathleen McGee: Indeed. I know we're going to talk a lot about that in another session, and I'm looking forward to that. Any last words of advice for our ... for our listeners?

Ken Fishkin: The last word of advice really is backups. And I think that it is so key to make sure that not only do you have backups, but you need to have backups of your backups so that where they are is somewhere where they can't be overwritten, because what hackers are doing right now is they're looking at your backups also, and they're overriding those as well. And it's really ... I've seen companies be decimated because their backups are gone. And so the idea is to either put it on tape, upload it to a service in the cloud–something that's not on your network. And that way, the hackers can't get to it. But too often, people get a little complacent, and they forget these things. They even

forget to test their backups, so they're not even sure that those backups even work. And, you know, they're, they're really in a hard position when they have to do ... when it comes to restoring. I've seen entire companies need to be restored from all the workstations, all the servers, soup to nuts, from a ransomware attack. And it is very scary. So if you don't have a plan to handle all that, then you might be in big trouble if that does happen to you.

Kathleen McGee: Well, I'm hoping that our little session today can give some people some food for thought on how to start taking stock of what they have.

Ken Fishkin: Absolutely.

Kathleen McGee: Well, I think we've covered quite a few of the basics here today. I'm looking forward to our next session. Thanks so much, Ken.

Ken Fishkin: A pleasure, thank you.