ESB: Erica Salmon Byrne
JW: Joan Woodard

This Week in the Boardroom brought to you by NYSE Governance Services Corporate Board Member, along with governance knowledge partners the Center for Audit Quality, and contributing partners National Investor Relations Institute and the Society of Corporate Secretaries and Governance Professionals.

ESB: Hello and welcome to This Week in the Boardroom. I'm Erica Salmon Byrne and once again we're on the road here at our Managing Third Party Risks event with section two of my session with Joan Woodard. I hope you had the opportunity to enjoy the first edition that Joan and I did cause we're going to dive right back into the material. So Joan, in the first set that we did, you and I were talking a little bit about the vulnerability aspect, the fact that really there's no industry that is not vulnerable to some sort of cyber security attack, that the vast majority of them go undetected for an extended period of time. As a director, what sort of activities should I be engaged in? What kinds of questions do I need to be asking my management team about to get a comfort level that they are on top of these issues? Are you seeing companies run breach drills? Are you seeing things along those lines? How extensive is this risk analysis getting?

JW: The first question that a board member needs to ask is what is my security? And I'll say not just cyber because physical security as well as personal security plays into this. What is my security policy and all of its parts, and what's the plan that we have, associated resources and the like? If the answer is a very narrow answer, here is our cyber policy, that's a good starting point for a director to engage very constructively because, as we mentioned in the earlier segment too, we think about cyber as largely the wires and devices, but in fact it is the human interface to that system that represents a significant vulnerability. So your personal training and personal policies are very, very important in having a very good strong system.

ESB: On the boards that you sit on, are you seeing a strong relationship between IT, Human Resources, Ethics and Compliance on those exact topics, or are we still operating in a world where those kinds of things are siloed.

JW: Starting. So, for example, one of the boards that I sit on just recently now has implemented workforce wide training, annual requirement for training in this area. And that has shown in the companies that have implemented that to be very, very effective. And this training is really addressing some of the most simple but most vulnerable aspects like making employees of the problems that can be created if they open a link in an email that comes to them that might be something suspicious. That simple awareness and think before one clicks can be a tremendous asset. So companies are starting to recognize that, but I think it is just starting. I've also seen the beginnings of connections between cyber and physical security because the access to your control systems for operational cyber risk as well as your access to the servers and the associated equipment in your systems is a very important piece.

ESB: Yeah. We have one company that we worked with that ended up engaged in the cyber issue because somebody had walked onto company property and randomly dropped thumb drives in the parking lot, and they had four or five employees who saw the thumb drives, picked them up, walked into the building, plugged it into their computer to try and figure out who it belonged to. So totally naturally human instinct to try to return it. And the very best systems in the world are only as good as the people are actually using them. So do you see directors asking questions of the management team around how they've operationalized some of their protocols? Are they testing them to make sure they're not getting in the way of the business? Because again, your system's only as good as the people that are actually going to use it.

JW: Absolutely. One of the clever things that I saw in doing this testing was actually a company that created spearfishing email templates and sent those to employees. And if they clicked on the link, which they weren't supposed to do, it would pop up and send them to additional training. And so it was a very gentle way of really trying to further bring to life for people and create that continuous awareness so that you have that important piece of defense in people.

ESB: And to go back to my original question about breach drills, are you seeing directors participate in those, ask about them? Is that becoming more and more commonplace?

JW: The asking about them and getting reports, after action reports from those drills, yes, I am starting to see that. Not so much participating in them. And some of those drills are actually cooperative drills across industry groups or cooperative associations of industry, so particularly critical infrastructure industries are doing more of that where they will do tabletop exercises. Another avenue is actually the Department of Homeland Security conducts national exercises, but those basically provide a general framework for the kind of thing that any company can do. And it is really important to run those sorts of exercises because when I think about cyber and general security, clearly your policy is very important. Having good practices across the board in terms of defending, protecting, responding, etc., but then the recovery and reconstitution so that you have trust in your system after an event is extremely important. And that recovery and constitution involves a number of different aspects. It's not just the technical system, but it's also communication both inside, outside to your board, to your stakeholders, to your customers to rebuild confidence.

ESB: Especially if you're a consumer facing organization. And we're seeing some of that now with some of the data breaches in the retail space. You're seeing those kind of those steps being taken. We're also seeing a lot of debate about regulatory responses. You know, in your experience, you mentioned the Department of Homeland Security and some of the work that's being done with the critical infrastructure organizations in particular. Is there a regulatory component here that you are hoping for or anticipating, or is the solution, particularly with third parties, going to be more about that we are going to incentivize our suppliers to be better and better business partners, and that's really how we're going to move the needle forward here?

JW: Yeah. I haven't seen that much in terms of regulatory yet on the third party side. There are some really good things, though, that are coming from the regulatory, and there are some areas I would just encourage companies to think before they necessarily act. The first is the NIST framework, the National Institute of Science and Technology framework. Though it was written particularly for critical infrastructure, is there really a good framework for any company to assess its maturity in terms of its systems and operations for cyber security, so.

ESB: And as a layperson who doesn't have a cyber security background, it's actually fairly readable.

JW: It is.

ESB: I was pretty impressed.

JW: It is, very much so. Another piece with regards to regulation, though, that I would just caution is that when an event happens there is, as I often say, we have a tendency in Washington to not do anything and then overreact, right? And that's true in a lot of parts of the country, not just government. But that overreaction will lead to requests for information that actually could be information that would reveal vulnerabilities. And so it's really important for companies to, working with their peers in the industry to, in fact, communicate and make sure that people fully appreciate either the vulnerability that's revealed or are able to work out some way to convey that information so it's protected. So that's very important to do.

ESB: And then the whole sort of theme of the conference that we're having here today has been this idea that working together with your vendors to identify the critical vendors who perhaps don't have the tools but want to have them and then those vendors who, for whatever reason, are just not in a position that they're going to be able to really live up to your expectations and figuring out how to extricate yourself from those situations. Do you see that trend accelerating, from your perspective, where more and more suppliers are going to be treating this issue much like quality was 20 years ago? Now quality is sort of a foundation, if you will, and you differentiate yourself on these other practices.

JW: No. In fact, I do. Again, in the critical infrastructure area, which has gotten a little more attention in this regard, some really good new practices that I've seen. One company actually has starting holding probably will be annual workshops. So as a critical infrastructure provider and perhaps a large one, those infrastructures are connected. They're networked with other smaller systems, sometimes other private companies, other public, municipal or cooperative infrastructure providers. These could be water systems, could be electric power. Those smaller entities do not have the resources. I mean a CSO, they could not afford to have a full time CSO. So having a workshop with them to give them awareness to just create a network so that if something does happen you have built in the relationships, the people relationships, to be able to respond to help them to push out solutions to their systems because you are only as good as the collection of all those entities together. So a very good thing. Same true for small business suppliers. Just as

we saw in the quality movement, small business suppliers, again, really didn't have the resources to bring in consultants and truly develop a very strong quality program, yet some of the simple basics in quality were easily conveyed and taught in sessions that large companies would offer. And so I'm starting to see that, which is a great connectivity, positive connectivity between the larger customers and their supplier base.

ESB: That's really interesting because I think for a lot of folks, myself included, you think about cyber security and your head immediately goes to a software answer or a technology answer, and so it's reassuring to know that at the end of the day it's as much about the people as it is anything else.

JW: Absolutely, absolutely.

ESB: Well, Joan, again, thank you so much both for your time today and then also for the panel this afternoon. Your insights have been most valuable, and I really appreciate you taking the time.

JW: Again, it's been my pleasure. Thank you, Erica.

ESB: And that is it for this edition of This Week in the Boardroom. We hope you'll join us next time.

Join us again next week for This Week in the Boardroom brought to you by NYSE Governance Services Corporate Board Member, along with governance knowledge partners The Center for Audit Quality, and contributing partners National Investor Relations Institute and the Society of Corporate Secretaries and Governance Professionals.

(End of recording)