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 on-the-road edition of This Week in the Boardroom. I'm Erica Salmon Byrne and we're filming today from our Managing Third Party Risks event here in Washington D.C. and it's my pleasure to welcome to our temporary studio Dr. Joan Woodard. Joan, thank you so much for being with us today.

JW: Thank you.

ESB: Joan, you obviously have a bio that I won't even try to summarize, but your current role you spend a lot of time working with boards and serving on boards. As a board member, our topic of course today for the panel that we're going to do a little bit later this afternoon, and then also for this edition of This Week in the Boardroom, is a director's role in cyber security oversight, especially as it applies to the supply chain. Why now on this topic? Why are we talking about this? Why is it so important?

JW: Well it's front and center on the news. Unfortunately virtually every day if not weekly we've read about large companies, small companies and the problems they're facing. And the thing that I find is most important for board members to appreciate is that a lot of these attacks, which have had substantial impact – retailers losing close to 50% in one quarter of time, year over year – is that it came about in many cases because of one individual and a third party vendor supplier of services to that company that unknowingly, possibly intentionally but most likely unknowingly, gave up their password and user name to allow access. That exposure that companies face today needs to be on directors' minds and to fully appreciate that it does not take a large breach of what they consider normally their defense in the cyber arena. It can be very small.

ESB: Right. That's one of the things that has really struck me about all the data breach research that I've read lately. At least in 2013, 100% of the breaches involved authenticated credentials. So there was a person failure in there somewhere, in some way, shape or form. And just so that we sort of set the stage for our audience, when we say data breach, what sort of data do I as a director need to be concerned about?

JW: Well that's a really good question Erica because in fact when we read a lot about the large data breaches...

ESB: Home Depot, Target.

JW: There's tens of millions of credit cards and debit cards. There's other aspects of data breaches which can be in fact small amounts of very strategically important information

to a company. It can be specific business details about business strategy or some new business action, merger, whatever, or it can be in fact design information that be lost. Example of a real case, a large company, global manufacturing company, lost, unknowingly they lost design information for key critical different shading products and only discovered that it was lost because of accesses they had given to a partner in another country to get into that market, but discovered it only after revenue dropped and then when they compared the details of the spec sheets for their product and this other company's product the comparison showed tremendous amount of identity theft.

ESB: You know I think that's one of the things that can make the data breach data conversation a hard one for a director to have because if you are having sort of that news headline driven conversation and you are not a consumer based organization, right, you don't have a ton of customer data, you're not gathering credit card information, it may be something where you think oh this is in that box, it's not me, but nowadays where 70% of the average company's value is intellectual property and intangible assets like reputation, data is data is data at the end of the day.

JW: Even beyond data. I mean there are aspects of the threat today that one need to think about on an operational side also. For example, I mean there, again a case, petrol chemical company discovered after a period of time that they were declining in revenues and _____ shipments of products only to unravel that and discover that there had been an outside tampering with their raw material supply automatic ____ system to cause that shortfall. And so one needs to think about the risk in a very holistic way. You need to think about your operation, understand the operation, and then start thinking a little bit from the standpoint of what would either competitors, you know a somewhat malicious competitor target in that operation, and then what would they find to be the most valuable if they were trying to, in fact, either take market share or enter into your market in a way. Another aspect is to think about okay so of your critical assets and are there activist groups that have a particular message or a message that they want to get to your stakeholders using what they might do to your reputation and your company. So by thinking in that perspective from the potential adversary's perspective, and taking a holistic look at your business, you can start getting a sense of where you may be vulnerable. The other thing is to always come into any discussion realizing you undoubtedly have already been attacked. The notion that we are safe because we have these great technical tools is no longer the case. So coming in with the mindset of okay we've been attacked but now the question is how significant and what are the early indicators of a potential attack that we might be looking for.

ESB: Let's stay on that early indicator piece for a second because if I'm the average director who hasn't had your level of experience with these critical issues, what should I be asking my management team about and what are some of those early detection factors?

JW: As they company is working these sorts of issues, one needs to gather what I call sort of risk intelligence on a continuing basis. One piece of that risk intelligence is by having some general idea of who potential categories of adversaries are, then look at what is the current activity data you're seeing, and there it is, in fact, thwarted attempts as well as

potential attempts. Where if you have a good system, you have a layered set of defenses, they may get through the first wall or the second wall. Those are important pieces of information to look at the total. The other aspect is what sort of monitoring do you have within your system today. The system is both the technical IT system, but also your larger business system, or what sort of monitoring do you have. Looking in the technical system, large exports of data. Those are very important indicators and where might you have vulnerabilities in entries into your system that you can detect from.

ESB: So those kind of almost dashboard reporting on those pieces of things is one of the things is one of the things that I'm going to get as a director that will allow me to have some comfort that my company has their hands around these issues.

JW: Absolutely.

ESB: And if I'm one of those directors that, you know, perhaps has a company that isn't gathering that information yet or I'm not seeing it, we're obviously going to do a two-part segment here because there's so much we can talk about – we're going to get into that breach planning and breach approach shortly – from a liability perspective, how scared do I need to be?

JW: My feeling is that there's virtually on industry today that should not have some healthy concern. Now, the concern should drive just starting questions about okay so what is our policy in this area of security and what is our operation, what's our plan, budget, staffing, and...

ESB: Who is my ____

JW: In particular exactly, who are the key officials? But also do we have operate that in such a way to be agile because this is a very dynamic picture and obviously in the event of another company in your same industry sector having a problem, one in fact needs to take quick action. So one company that I worked with had something called pop-ups in their budget where through the year they have a small amount of money and a mechanism to get more resources, but as issues and opportunities to work those issues come up they do a pop-up and that allows them to be very agile on moving forward.

ESB: So if there was an issue in their organization, of if there was an issue in their industry, if a peer, if there was a disclosure related to something happening to a peer, they would access that pop-up to address that particular issue.

JW: Right, right.

ESB: Terrific approach. Well now that we've scared the pants off our audience, we are going to go ahead and pause here because we have so much more we can talk about. But we are out of time for this particular edition so we're going to pick this up in just a moment. I'll thank you twice, so let me thank you for the first time. Thank you so much for taking

the time to be with us both for these two editions of This Week in the Boardroom and for the event today.

JW: It's been my pleasure.

ESB: And thank you for joining us for this edition of This Week in the Boardroom. I hope you'll join us next time when I pick my conversation up with Joan and we're going to talk about how a director can be adequately prepared for a cyber security attack.

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)