uberknowledge

Jake Olcott, VP, Communications and Govt. Affairs, BitSight

What Are the Questions We Should Be Asking?

Jake discusses the cybersecurity questions we should be asking: what legislators should be asking citizens; what boards should be asking CISOs; what companies should be asking during M&A processes; and what citizens should be asking themselves.

03:22	While it's true that legislators lack technical knowledge, the best ones know how to ask the right questions.
04:49	Americans need to consider if they want Europe to be setting the privacy regulations and if not, they need to ask U.S. legislators to start doing so.
09:03	Boards and executives are on the hook for cybersecurity and finally understanding that it is a critical component to an overall risk management program.
13:54	The Marriott breach showed cybersecurity diligence during M&A is essential.
15:49	The goal for CISOs with any breach is to learn from it, develop the appropriate standard of care, and then show those learnings to the executive team.

Ashwin Krishnan: [00:00:30] So we're at RSA 2019, and with me I have Jake Olcott from BitSight. Jake, good to have you on this podcast.

Jake Olcott: [00:00:39] Thank you. Good to be here.

Ashwin Krishnan: [00:00:40] So before we dive in, for the sake of our audience, you have a diverse background in academia, business, and as a security vendor, right?

Jake Olcott: [00:00:49] Yes.

Ashwin Krishnan: [00:00:49] So, from your perspective, how does having that kind of diverse background help you become a better vendor? I mean from a 360-degree perspective. Then just give us a little bit of your background.

Jake Olcott: [00:01:02] Yeah. I probably have an unconventional background when it comes to working in the security technology space. I always tell people I'm a history major and a lawyer, and that's the view that I take when I think about cybersecurity. For years I've been working in cyber. I've sort of taken that kind of legal and policy background to try to understand some of the key problems, maybe the historical challenges that we've had. How can we apply things that we've learned in other backgrounds and experiences? How can we apply that to cyber which is, of course, a new risk? But we do have a history of risk management, so how can we bring some of these practices, economics, history to bear here?

[00:02:01] And so personally, I spent a number of years working on the Hill. I worked in the House of Representatives and the Senate. I worked as a consultant for a number of years. But I have been exclusively focused on cybersecurity and cyber risk management in all of those areas.

Ashwin Krishnan: [00:02:20] OK, so this is the first time I have a podcast guest who has actually worked on a Senate committee. Given how front and center technology is today, whether it comes to Zuckerberg being on Hill or Sundar Pichai or whoever else there is … I'm quoting the media here because, as a lay person, I don't know the woeful lack of understanding of technology when it comes to legislators and congressmen and congresswomen — especially so when compared and contrasted with Europe, where they have chief privacy officers and the government is really aware of what's going on. So, given your vantage point and your association with where the U.S. is, are we at an inherent disadvantage because of historical reasons, given your history major, or do you think that we're going to be catching up very, very quickly? Just given the fact that this is existential right now.

Jake Olcott: [00:03:22] So I would say it's a great question. A couple of different observations. First of all, I am just as frustrated as everybody else. You know, I had the benefit of working with a couple of really great legislators, Congressman Langevin, who is known in the House of Representatives as being a great leader on cybersecurity policy issues. I worked for Jay Rockefeller in the Senate, on the Senate Commerce Committee, who's also a forward-leaning person. And, you

know, the way I would describe those two legislators, they were interested in understanding what was going on and recognize that this is a big challenge. They didn't feel the need to be very technical, but they knew how to ask the right questions.

[00:04:28] And what's interesting is that when I think about cybersecurity today, there's so much emphasis that we're placing around senior executives and board members being responsible and accountable for these things. People have been trying to say, "Oh, the C suite needs more cyber expertise and the boards need more cyber expertise." I actually don't think that's necessarily true. I think that they need to be asking better questions. And so that's just the way that way that I'm thinking about this.

"The question, as American citizens, is, do we want the Europeans to be doing that for us?"

[00:04:49] Now, your question, Ashwin, about what's happening in the U.S. compared to what's going on in Europe, I think what we see is that the Europeans are really setting the standards in a lot of ways for the way that organizations think about cybersecurity and privacy. The question, as American citizens, is, do we want the Europeans to be doing that for us? Do we want our legislators to be doing more for it or something different? And ultimately, the question is, if we want something different then we really need to be asking them to do something different. And what they're hearing today in large part is that there's no real demand. I think there's concern from the average American citizen, but they're definitely not banging down the door of their legislators to do anything about it. Unlike in Europe, where privacy is part of the DNA of the citizen. It's just a very different environment.

Ashwin Krishnan: [00:05:57] So that's a great observation. And I'll just throw in my own observation over here, talking about citizenry and the awareness of privacy. I think it was at the CSA summit yesterday that there were a few observations being made by panelists suggesting that most organizations, or at least the forward-leaning ones, are treating everybody like an EU citizen when it comes to GDPR and compliance because it's the right thing to do and it's easy.

[00:06:27] But on the flip side, there's also, and you might agree or not with me here, there is a cognitive dissonance that I've seen in tech-minded people. They go to work, and they do business as a businessperson, whether it's like you said setting up product roadmaps and customer conversations and so forth, but when they come home, they pretend they are a dumb consumer. And if they figure out that Alexa has been listening to their intimate conversations, they feel they have the right to be upset now. So the question I have for you is, yes, on the one hand, we pretend as American citizens that we don't really care much about privacy; on the other hand, we feel the need to feel upset and get angry at Google or Amazon, if something bad were to happen. So the question is, are conferences like these raising awareness, not just at an enterprise level, but as a consumer — I don't want to use the word activist consumer — but an aware consumer and do

you see that playing out?

Jake Olcott: [00:07:33] I think it's a super question. I have actually been coming to the RSA conference for a number of years, and, you know, it's always a great conference catching up with old friends and seeing what's new in the market. I'm actually not sure that people bring some of the things that they're becoming aware of back to their own lives. I do wonder if some of the other conferences that are a little bit more hacking focused — you know, I can hack a watercooler or a coffee machine — I wonder if that does more for the heightened awareness of the individual consumer than a conference like RSA.

Ashwin Krishnan: [00:08:27] Right. So, you've been public about how to answer the question every board in the industry wants to hear. And the question is, how does our cyber-risk level compare to our peers and compare to where we were last year? So back to your earlier question about how does the board start asking the right sets of questions without getting, like you said, a tech head or a cyber geek. Is risk and trust and privacy ... I mean, what sorts of questions would you, Jake, recommend that a board member needs to start asking?

Jake Olcott: [00:09:03] Yeah. I think most of us are appreciating today that senior executives and board members are on the hook for cybersecurity. They are starting to understand that it is a critical component to an overall risk management program. The question is, what do we do about it; how do we think about it? When you think of senior executives and board members specifically, the role there is to establish the right governance programs, establish the right framework, the strategic framework for the way that the organization is going to tackle this problem, tackle this challenge.

"It is a critical component to an overall risk management program."

[00:09:44] Boards are really there for oversight. The role of the board member is to oversee what has been established by the executives with respect to risk management. And what's interesting is that board members play a crucial role in asking those fundamental questions about have we established the right strategy when it comes to cyber risk? When you think about that, it's a question of what are we focused on? What are we protecting? What data is most critical for our organization — commonly referred to as the crown jewels — how are we approaching this challenge? Do we have the right people? Have we hired the right people?

[00:10:39] From a financial standpoint, what are we getting out of our program? We're spending more and more money. You know, when I think about the conference organizations really taking advantage of what has been an open checkbook for many years. Board members just, you know, writing checks left and right, "Hey, whatever you need, you can buy."

[00:11:03] But they're really starting to think more about that. Just what are we

getting? What about how we measure the efficacy of our program and our spend. But ultimately, what the board really wants to know is a very simple question, which is, how are we doing? How are we doing? And what's interesting from the CISO and CIO perspective is that for years it's been very difficult to communicate the answer to that question in a way that is meaningful for a board to understand. Because boards want to know not only how are we doing, but almost as important is, how do we do compared to our peers.

[00:11:48] There's always been, I'll put my legal hat on for a second, there's always been this conversation about the standard of care in cybersecurity. What that means is, you know, what are we supposed to do? Are we achieving that? Are we in line with what others are doing or not? The answer to that question really lies in understanding your own security performance, the peers and competitors in your sector, how they are performing. What makes cyber so challenging and so interesting is that, that performance is dynamic. Things constantly change. And so, to be able to answer that question, that fundamental question for the board, you have to be able to answer in a dynamic way.

Ashwin Krishnan: [00:12:32] So let's dig a little bit deeper. Just take the Marriott breach right now, over 500 million records or something to that effect? So if I am on the Hyatt Board or Hilton Board right now, what questions should they be asking of their executive team in order not to be the next Marriott? Or is it more of saying, let's do a little bit more than Marriott did, so we don't get dinged? Are you seeing the bar being raised to, let's do the right thing by the customer, or let's just do better than our nearest competitor so that we don't get dinged?

Jake Olcott: [00:13:12] It's a super question, and I think it definitely depends on the organization.

Ashwin Krishnan: [00:13:16] Right.

Jake Olcott: [00:13:17] You know, organizations are competing on security. That is absolutely happening. By the way, five years ago, you might not have been able to say that. That might not have been true. But with so much attention and focus on this idea of third-party risk and trying to assess and evaluate my vendors, you know, the organizations that are doing business with me now, if you're a vendor today, which every company is, you really have to think about security as being a critical factor in the way that ...

> "Organizations are competing on security."

Ashwin Krishnan: [00:13:54] You get assessed.

Jake Olcott: [00:13:54] Exactly right. It's price and ability to deliver the service and security that's really part of that process.

[00:13:57] From the Marriott perspective, so many interesting things happened in this incident. And actually, I look at the Marriott breach as ultimately a failure in the M&A diligence. I mean, when you think of the idea of acquiring an

organization like a Starwood, what are the questions that we need to be asking of Starwood about their security performance and their security posture? How do we assess that and measure that? Anybody who's ever done an M&A diligence or even a vendor diligence realizes there's a lot of things that you need to be asking of the organization. Of course, sometimes the organization will share some things with you, sometimes they won't.

Ashwin Krishnan: [00:14:57] So let me quickly interject. Do you think that cybersecurity diligence during M&A is raising the overall M&A risk posture, saying we now need to add these three questions, these three process subheadings in every M&A transaction, regardless of whether it's the hospitality industry or the retail industry? Or is it another footnote in history, where Marriott is gone, let's go back to business?

Jake Olcott: [00:15:30] I think that if you are not adding security to the M&A process today, you've completely missed the boat. First of all, you missed the boat a while ago, but that was one of the key takeaways from the Marriott breach.

"If you are not adding security to the M&A process today, you've completely missed the boat."

[00:15:49] You know, going back to what the board is thinking about, what senior executives are thinking about, the goal — for the CISOs and CIOs who are listening to this and thinking, what should we be doing next — the goal when any public breach like this happens is you've got to be able to take some nuggets from that event, incorporate into your own program, and be able to go back to your senior executives and board saying, "Look, these were a couple of things that I've learned from this. This is how we've changed the way that we think about this." And so, we're constantly learning, and that's true not just if you're in the hospitality industry. You have to be able to look at Marriott if you're in the financial sector, electric utilities, retail, etc.; everybody is acquiring something. So I really think that's a huge missed opportunity, if you don't do it.

[00:16:50] The other interesting thing is that because everybody knows about what has happened, it's all part of building that appropriate standard of care. So if you didn't do it before, everybody knows it now. And you don't want to be the one months or years from now, who wasn't doing the thing that everybody agreed was the right thing to be doing.

Ashwin Krishnan: [00:17:11] So that's a great way to kind of end the conversation. I just want to ask you one more thing: from Jake's perspective, what would success at RSA 2019 look like?

Jake Olcott: [00:17:24] Great conversations with friends, great conversations with customers and prospects. This area of cyber continues to be so interesting and fascinating. It's all about risk management. One of the things I've been really happy about with the evolution of this conference is we're increasingly focused on

risk management as opposed to just straight-up security. And I think it's a really positive development. We've got to be better about thinking about it in those terms. So being able to kind of carry that conversation forward, it's definitely something I'm looking forward to this week.

Ashwin Krishnan: [00:18:06] All right. Thanks, Jake, for an awesome conversation. Hope the rest of RSA turns out to be as insightful and fruitful as this.

Jake Olcott: [00:18:15] Thank you, appreciate it.