Podcast Transcript

The Data Stream: Episode 12 with Ben Wanger

Date: September 3, 2026

Guest: Ben Wanger, **Host:** David Sherman, Nichole Sterling

Run Time: 24:23

For questions and comments contact:

Benjamin D. Wanger

Partner
Philadelphia
T: +1.215.564.1601 | bwanger@bakerlaw.com

David Sherman

Partner
Philadelphia
T: +1.215.564.8380 | dsherman@bakerlaw.com

Nichole L. Sterling

Partner
New York
T: +1.212.589.4282 | nsterling@bakerlaw.com

May: Welcome to the Data Stream, the podcast that dives deep into the fast-moving currents of data, technology, and the law. BakerHostetler's Digital Assets and Data Management Practice Group brings you this series, hosted by partners David Sherman and Nichole Sterling, to explore how companies navigate the complex and often intertwined life cycle of data, privacy and cybersecurity, to advertising, AI, and other emerging technologies. I'm Charlie May and you are listening to BakerHosts.

On today's episode, David and Nichole speak with Ben Wanger. Ben is a partner on BakerHostetler's Digital Risk Advisory and Cybersecurity Team and the co-leader of BakerHostetler's Multidisciplinary Industry Group serving educational institutions. Ben has significant experience helping educational institutions develop data breach prevention and response protocol and respond to data security incidents.

Sherman: Ben, thanks so much for joining us. To start, you've built a significant part of your practice around representing educational institutions. What drew you to that sector and what's kept you there?

Wanger: Well, thanks for having me. I really appreciate you guys having me. I think there's really three main reasons that drew me to the education sector and that made me stay. The first is I just enjoy universities. I enjoy college campuses. So, I think being interested in universities and how they operate is something that really did draw me initially to working with universities in the cyber context. I think another thing about universities that I really enjoy is there is this chaos in universities where a lot of normal companies, they're very, I would say vertical, where there could be a CEO, then there is a vice president and it is very much a up the ladder where you know who is in charge at all given times.

Universities have this, I would say chaos and they're very horizontal in their leadership where everybody is these co-equal authority figures trying to figure out how to make something work. And I think in the context of a cybersecurity incident, there is a lot of chaos in that nobody really knows whose job is what. So, there is really a need for someone like me to come in and help run their incidents and help work across functions and make everything work right. Because I think the need is something, like I said, that drives me to it.

The other thing that drove me to it was, just to be blunt, there wasn't anybody else that I saw in this space who was making educational institutions their focus. So again, in my career where I enjoyed working with them, I knew a lot about universities, and I just saw a space where there wasn't anybody else doing it. So that is what really drove me is that I was saying I could be the guy who really understands that these cyber incidents as they impact universities better than anybody else. So that was really a motivating factor as well, just the opportunity to be probably the guy with no equal really.

Sherman: So, Ben, I think you just touched on this a little bit, but when an educational institution suffers a cybersecurity incident, what makes the response for a university or a college or even a secondary school significantly different from any of the other corporate incidents that I know you handle?

Wanger: The biggest difference is just the spread out governance. Is that, for example, in many universities I work with, you'll have the risk management group, you'll have the legal group, you'll have the IT group. And oftentimes they don't even talk that much. So, a lot of what I'm doing is working across groups to make sure that everybody is on the same page and nobody's feelings get hurt afterwards. And really making sure that everybody can work together because frankly, oftentimes

they haven't practiced working together and that is not a thought. Everybody is in their own silo within this university world. That is a really big thing.

Also, unlike a lot of other companies where they very much know exactly what is going on in all aspects, they know HR is doing this, sales is doing that; universities are very different in that nobody really knows what anybody else at a university is doing. You have people doing research that legal or risk has no idea what kind of research they're doing. They don't really even always know where they're keeping their data. So, there is a lot of finding out what data you have because unlike a lot of other core entities, universities really don't tend to know exactly what data they have and what everybody in their system is doing. They're not like some companies where everybody is really pedaling in the same direction. In universities, everybody is going different directions doing their own thing. And that makes it very difficult when you have a cybersecurity incident from the context of figuring out what data was involved and then figuring out how to make sure that we're identifying all of the potential avenues of access and what went on in the network. You couple that with universities have a ton of data, whether it is student data, whether it is employment data, whether it is research information, whether it is healthcare information. I mean, universities have every kind of data that is imaginable all in this one entity.

Sterling: So, we basically have a bunch of siloed ivory towers going on at the university level.

Wanger: And that is not to mention that universities also teach students. So, while we're worried about all of these operations, we could also be worried about, well, we have class that is going on tomorrow. We're going to have to cancel class. All the while you have a student newspaper who is trying to figure out what is going on. So, I mean, literally everything that could possibly happen in one incident or in many incidents is all combined into this one incident.

Sterling: Sort of a microcosm of the real-world incident, but you have everything from your media to pockets of data that nobody has even looked at. And I think one thing we wanted to ask about really, you mentioned student information. And of course, on the privacy side of things, we often work with children’s data and know that is a particularly sensitive category, but student information more broadly, including university student information can be uniquely valuable, it seems. What makes it uniquely valuable or particularly difficult to protect in this context?

Wanger: I'm not sure that I would say student data is necessarily uniquely valuable. I mean, there is a lot of it. So, there could be data, I mean, there is data that could be sensitive to a student, for example, information about their grades, disciplinary information. I mean, there are a lot of information that a university probably has about a student that the student wouldn't want getting out there. And the university generally doesn't release that data for one of several reasons. So that type of data really could be problematic if it gets out. But in general, a lot of the data that they have about students that really we are worrying about, and I’m sure you’ve noticed, it is the same kind of data that other entities have.

Your PII, like social security numbers, there is obviously FERPA data. FERPA is interesting in the context of data breaches though, because FERPA does not require you to actually give notice in the event of a cybersecurity incident. So, and just to step back, when I talk about FERPA data, FERPA data really refers to any part of a student's educational record. So that would be grades, the classes they took, financial aid information, any records that a university is compiling about a student is considered FERPA data. Which exempted from that is what they call directory information, and that is really phone book information about a student. So, a student's name and phone number or e-mail might not be FERPA because it is directory information and easily accessible, but everything else is considered FERPA data.

FERPA, though, does not require any notice in the event of a cyber incident involving that data. What it does require is just some note in the student's record basically indicating that there was an incident involving an unauthorized disclosure of that data. And the student would see that information if they ever request a full version of their student record but otherwise, there is no reason that a student would ever even see that and find out about it.

Sterling: Got it. And just for clarity, I'll throw in that when you talk about FERPA, you're referring to the Family Educational Rights and Privacy Act for people who are not quite as used to our acronyms.

Wanger: That is correct.

Sterling: Yes. So, looking at educational leaders across the board, what do you think they most often underestimate about cyber risk?

Wanger: I think what they most often underestimate about cyber risk, well, first of all, they underestimate the problem that keeping every piece of information and data that has ever come into possession of the university could cause. I think a lot of people think that, let's just keep everything so that way we'll never be in a situation where we don't have something. But they don't think about how that could add to their exposure. Meaning if you keep every social security number of every student that is ever attended your school, and then you have some cybersecurity incident, well, you're just adding thousands of people to a potential class action that is brought against the school. So, I think that is a big deal, the idea of retention and deletion. I will tell you that, I mean, something I've been talking to a lot of schools about are their document retention and deletion policies. And I will tell you more often than not, a lot of schools I work with have very nice, fancy document retention and deletion policies that they pretty much don't give any thought to after they finalize the policy. In other words, they have the policy, but their compliance with the policy is almost non-existent.

The other thing that I think the schools really underestimate, and I think this also applies to non-schools as well, but the importance of practicing the incident response process, meaning you can devote as much money as possible to a great, to a very robust cybersecurity defense program. But in this day and age, I think it is inevitable that you can't prevent every cybersecurity incident. And I

think especially the large universities with really spread out shared governance need to practice, what is it going to look like if we have an incident? Who is making decisions? Who needs to be involved in those decisions? Because I see very often there is confusion about, again, how decisions get made, what the process is, and whose input really needs to be taken into account.

Sherman: I want to follow up quickly on something you just said, which was really interesting, meaning we have all of these university and higher ed clients generally with these really robust information governance policies, data retention schedules, et cetera. And I know one of the things that you and I see very much eye to eye on in the context of incident response is not letting a big crisis go to waste. Would we be better served if at times we pressed universities to try and use some of those policies that they tap to say, we have gold standard information governance programs or retention schedules, et cetera, to press them and see how they actually help clients understand risk to data in the context of a live incident. Have you ever done that before? Or if not, perhaps we, just thinking aloud, maybe we should really use this as an opportunity. What do you think?

Wanger: I mean, I talk to clients about things like that all the time. And the position that I normally take is a policy is only as good, as helpful it is going to be when you need it. Meaning, if the policies that you have in place aren't helping you, you're not following them, they're really not helpful to you. And sometimes, frankly, it is better to not even have a policy if you're not going to follow it. But I think to your point, yeah, I think especially in universities where to do anything oftentimes you need to get buy-in from several levels of authority. I think, and a lot of times when the school has a cybersecurity incident, you're right, you don't let a good crisis go to waste. That is really the time for them to capitalize and making sure that the higher ups see how important these issues are, how important it is to have a policy that is good and you're able to comply with and make sure that you're putting in the investment at that time, because that is when you get the most buy-in.

Sherman: Yeah, makes sense. And to that end, as we think about not just governance, right, but technology stack and where risk really lies, right? Universities are often focused, at least from my limited experience, on their literal footprint, right? Meaning, well, we have, the following on-prem systems and we outsource the following to the cloud. Do you think that as university or higher ed tech stacks evolve and continue shifting towards the cloud, that the largest risk vector remains on-prem? Or are we seeing TPRM and vendor risk become the primary risk vector for higher ed?

Wanger: You're right that universities, like a lot of entities, are moving more and more data off into the cloud and off the on-prem systems. What I keep seeing though for these systems, is the data that they're moving is not data that is ultra-sensitive. It is a lot of data that could be covered by FERPA. It is data that is, a lot of it is phone book type data. Some of it is academic, but it is not data that is triggering notice. I mean, in the education world, we had this breach of a learning management tool called Canvas over the summer. I guess it was the spring into

the summer. And almost every school uses Canvas. Canvas is one of those tools that almost every school uses as a learning management tool. There is tons of data that Canvas hosts from almost every school. Me personally, I've probably spoken to over 50 universities who were notified by Canvas that their data was involved in this breach that Canvas had. And I will tell you, thus far, I have not had one university that has had to actually provide notice under the law in connection with this incident. Because all of the data is learning type data, but not data that would include social security numbers or other type of information that would actually trigger a legal notice obligation. So again, while you see schools moving more and more information into the cloud, that is not the information that really is creating the most exposure for them.

Sherman: Interesting. You just said something which caused me to have a chain of thought moment, if you will. As we think about the vendor landscape, right, and outsourcing information and university culture, right, again, I recognize, and you and Nichole probably know this far better than I, but that universities have particular security challenges surrounding access to information, given how openness is really part of their mission, right, in terms of research collaboration and academic freedom and international engagement. And again, just having access to open networks and systems are, I think, culturally integral to university operations. But as you just mentioned with Canvas, right, where we have, you're talking to 50 clients or 50 plus clients about a platform that hosts fairly non-sensitive but broad-based information. How do we remain respectful of what makes a university a university while also adopting more robust security practices like tightening identity management controls for some of those vendor systems, for instance?

Wanger: I guess I see it a little bit differently. I almost, I mean, obviously universities have to be managing their vendors. I mean, we've seen time and time again these vendor incidents. I mean, other ones like MoveIt, Accellion that have caused much bigger problems for universities where they have needed to end up providing notice. But I almost think the Canvas incident shows is a success in that the universities were making sure that the data being shared with Canvas was data that was not ultra-sensitive. So, I almost see it as a success on the front end for them making sure that the data that they are sharing here and the data that they are putting out there is not data that really brings with it a great deal of exposure for the school.

Sherman: So, what you're saying is that if they're more mind, right, if universities are more mindful about how they're uploading or ingesting or processing information in the cloud, then that itself both respects their mission and also enhances the viability of their security program.

Wanger: Yeah, I think being very careful about who you're sharing information with that actually could bring exposure with it, I think that is something that I would be focusing on if I were a university.

Sterling: Alright, before David takes us on too many other detours, I get to take us on a detour. Since we are talking about universities, campus culture, back to school

season, et cetera, we have to take a brief Michigan detour. We know, Ben, that you bleed maize and blue, despite working for an Ohio headquartered firm. And Michigan is entering this new football season with new coaching staff and a lot of attention on how this program will evolve. What are you most hoping to see from the Michigan football team this season?

Wanger: I am most hoping to see them get back to the way that they should be with beating Ohio State and keeping my fall Saturdays full of hope. Getting me to Thanksgiving with hope of a national championship is pretty much all I can ask. But yeah, I mean, the Michigan fandom has brought me a lot of insight into universities. I can tell you that there are many universities that I would probably would not have been to if I were not traveling to them just as an opposing football fan. And I probably would have a much different view of them if the first time I had stepped foot on them, I hadn't been being yelled at and told how awful I am and how much I suck. But I still love them anyway. No, I'm just looking for a fall full of hope and hopefully just beating Ohio State again.

Sterling: Alright, so looking at that, we have to say that Michigan's schedule, myself also being a Michigan fan, I've looked at the schedule. It is pretty brutal this year. We've got everything from Ohio State to Oregon, Oklahoma, Penn State. What do you see as the realistic floor and ceiling for this team's record?

Wanger: Their schedule is tough. It is hard to say with a new coach, but I think they're going to take a jump with Bryce Underwood, the sophomore quarterback. I think they're probably a three or four loss team and in this kind of era of college football, the difference between being a three-loss team and a four-loss team is huge. I mean, that generally is the difference between making the playoffs and not. I think they're probably a four-loss team, but I think if everything goes right, you could see them maybe only losing two of their first games. I mean, frankly, all you can really ask for if you're a Michigan fan is that you go into that last game of the year against Ohio State with an opportunity to move on if you win. That is probably the best-case scenario for Michigan is that when the Ohio State game comes around, they're playing for continuing their season as opposed to just going to one of the no-name bowls.

Sterling: So, is there a particular early season game that you are keeping an eye on that you think will give us a good, I guess, insight into what we might realistically expect from the team?

Wanger: Yeah, Michigan plays Oklahoma in the second week of the season. I know when I was in school, we usually played pretty easy games to start the season. But when you have Oklahoma the second week of the season, you don't really have the opportunity to ease into it. So, you'll know what you have in Ann Arbor pretty early on. And I think if they can beat Oklahoma in week two, all the expectations will shoot off. And I think that would really determine where the expectations are. Until then, you really don't know what you have. But once you play Oklahoma in week two, if you win, then you're talking about a possible, if not likely, playoff berth. But I think that'll tell you everything you need to know about where this team is headed.

Sterling: So, there we go. Second week of the season. We'll know exactly how Ben is feeling.

Wanger: Yeah, exactly. You'll know very much how Michigan did when I come in to work on Monday the 14th.

Sherman: Fair enough. Well look, to wrap this up, as we think about education more broadly, if you could give every district superintendent, university president, university GC or CISO, CIO, et cetera, one practical bit of advice related or unrelated to football, perhaps cybersecurity for the next year, what would it be?

Wanger: Practice. My number one piece of advice is, first of all, you have to practice. You have to practice the incident response process. Make sure you know who is in charge, how decisions get made. I can't tell you how often I hear from clients, wow, this really opened our eyes to how the process works and we're going to be more prepared next time. So, I'd much rather my clients be prepared the first time and not need an incident in order for them to have a feel for how the incident response process works. So again, I think practicing the incident response process is vital and pays extreme dividends in the event of an incident.

And I would also say that I think in higher ed, the word transparency is pushed around a lot. People talk about how important it is for these schools to be transparent with their community, with their students, with their employees. And I think, I didn't mention this before, but in this day and age, I think having a cybersecurity incident really does not necessarily do significant damage to a university's brand. I mean, the truth is that enough schools have had these incidents that they're just not as uncommon as they used to be. But I think the way a school messages about these incidents and the way they release information has a huge role in determining whether the incident is just a blip on the radar and the school is just lumped with one of many who have had some kind of incident or the school becomes the butt of a joke and people start criticizing the school for not knowing what it is doing. So, I think schools really need to make sure that they're balancing the need for transparency with the need to make sure your communication plan in the event of an incident is very tight and not bringing about more questions or giving the opportunity for you to look foolish with how you message about the incident.

Sterling: So essentially they need to practice a lot. And of course, Ben, you are willing to help them practice. I know this is something that you do a lot of. So, I will just throw that out there. If anybody needs help, feel free to call Ben. Thank you very much for joining us today. Great to hear a bit more about your educational cybersecurity practice, which honestly I don't think I've heard a ton about in the past.

Wanger: My pleasure, guys. Thanks for having me.

Sherman: Thanks, Ben.

May: If you have any questions for David or Nichole, their contact information is in the show notes. As always, thanks for listening to BakerHosts. Comments heard on BakerHosts are for informational purposes and should not be construed as legal advice regarding any specific facts or circumstances. Listeners should not act upon the information provided on BakerHosts without first consulting with a lawyer directly. The opinions expressed on BakerHosts are those of participants appearing on the program and do not necessarily reflect those in the firm. For more information about our practices and experience, please visit bakerlaw.com.