Podcast Transcript

Universities and Cybersecurity Incidents

Date: September 17, 2025

Guest: Benjamin Wanger, Paul Davis, and Tom O'Neill **Host:** Charles May

Run Time: 26:46

For questions and comments contact:

Benjamin D. Wanger

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

May: Just like businesses in other industries, higher education institutions across the country are dealing with cybersecurity incidents. Knowing what resources are available during the incident planning and response phases is crucial for these schools. I'm Charlie May, and you are listening to BakerHosts.

Today, Counsel Ben Wanger from BakerHostetler's Digital Risk Advisory and Cybersecurity team is joined by Paul Davis, the area senior vice president and regional director at Arthur J. Gallagher and Company, and Tom O'Neill, management liability and cyber practice leader for Assured Partners, to discuss these cybersecurity resources.

Wanger: Paul and Tom, I'm really happy that you guys are joining me today. You guys are obviously two of the most active cyber insurance brokers in the education space. I know I've presented with both of you at conferences regularly, most recently with Tom at the SUNY Technology Conference. And one thing that I always see when we are presenting together and we're speaking to universities or other audiences is, a lot of our talk is you guys are keying me up to talk about the incident response process. I thought it would be fun today to take the opposite approach, where we'll talk about the incident response process, but more from your perspective than mine.

Paul, why don't you start? Talk about your relationship with the school clients that you work with. What do you really do for them?

Davis: Yeah, thanks for having us, Ben. It is a pleasure to be here speaking with you and Tom. Yeah, I mean, as you well know, cybersecurity is not just a once-a-year type project for higher education institutions. It is a true year-round project. Data

privacy doesn't end when we renew a policy. At Gallagher, we really want to be more than just a placement broker and be a true cyber risk consultant for our clients. So, some of the things that we do throughout the year, we'll do an onboarding meeting with our clients after we place the program and advise them of some of the complimentary and discounted services and products that are offered by their insurance carrier. We'll also advise them of the coverage triggers for their policy, who their approved incident response vendor panel is, and so they can really maximize the benefits of their insurance program. So, that is a good example of one additional touch point that we have with our clients throughout the year.

Another quick example I'll throw in there too is we speak with underwriters on a regular basis about what cybersecurity controls are most important to their underwriting, and we produce a report once a quarter that we share with our education clients about, and we prioritize that list of cybersecurity controls. And a lot of our clients really appreciate that list because it helps them prioritize projects within their organization when funds, headcount are limited, and their attention is pulled in many different directions.

Wanger: Ben, I know I work with a lot of universities in the cyberspace, and I know that there are certain aspects of universities that are just going to make them very unique to deal with. From a brokerage perspective, Tom, how are education clients different than others? Why does it require some expertise to work with these educational institutions?

O'Neill: Yeah. The education space is unique, I think, from a business organization standpoint but also from a network construction standpoint, right? So, with a university, you're going to have separate networks for students. You're going to have a guest network that is hopefully segmented from the rest of the network. So, just given the number of users that can be accessing one of the college's or university's networks at any one time, it does create a unique exposure. That combined with the potential threat that threat actors are going after the higher education space, yeah, higher ed certainly has their work cut out for them from a network security standpoint.

Wanger: Great. So, let's talk about cyber insurance coverage. From your perspective, what should schools, universities and K to 12 schools, what should they be looking for in a cyber insurance policy, Tom?

O'Neill: Yeah, I think the biggest thing there is you need a policy that aligns with your incident response strategy. So, you need the right coverage with the right limit and the right carrier. And I think that the, one of the best examples for hitting that sweet spot for the right coverage is by selecting a policy that is going to align with how you are going to respond to a cyber incident. And basically, you have two options for how you can set up your cyber policy. You can use the incident response panel vendors that your carrier has pre-established as the carriers or the response vendors that they work with on the legal side, on the forensic side, and you can use those firms. And you may decide that you want to pre-establish

a relationship with those firms, or maybe you just want to go with who is available at the time. But that is Option 1.

Option 2 is you structure a policy where you work with your carrier to pre-approve a forensic firm or a law firm, and you schedule that firm and their rates on your policy. So, two very different strategies, and it is important to decide which avenue that you want to go with when you set up your policy. When you renew your policy is the time that you have to establish which of those two options you're going to go with.

And there is value in each direction. Of course, with the value of working with a panel vendor is that these are the top firms who do this stuff every day. They're pre-negotiated rates and usually the vendors, the law firms, the forensics firms, the ransom negotiators, they all have been handling so many cases together that there is a lot of symbiosis. There is a lot of good teamwork from those folks. Obviously, seeing that, Ben, with the way that you work with the various forensics firms and the ransom negotiation firms when you handled incidents for our clients.

And then it may be that you have decided to, that you need to use a particular forensics firm or you need to use a particular incident response law firm. And if that is the case, then if your cyber carrier does not have them on their panel, then you need to think about how you structure a policy so that you can work with the vendor that you want to work with and still have bills paid for.

Wanger: Yeah, I think it is a really interesting point, talking about how you want to make your incident response policy or plan first, and then find an insurance or cyber insurance policy that fits that plan. I think you probably see it much more the opposite, where you'll see a school get their insurance and then find a plan that fits their insurance, but you could probably have the best of both worlds if you make that plan first.

O'Neill: And unfortunately, more often than not, it is the universities who have gone through an incident and who have gone through a claim who are taking the proactive steps in how they set it up for next time. So, if you can learn from other universities' unfortunate situations, then you'll be best set up and best prepared for an incident as you work through that.

Wanger: But one of the things that I've seen in the incident response process, and I think everybody knows, is the vendors that you choose, the legal vendors, forensics, play a very large role in how successful the incident response process is. I agree with you 100% that identifying them in advance is very important because that is how you can make sure that you're going to have the best possible help. But Paul, what does that process look like if there is an insurance policy that generally fits a school's, it fits everything that they want, except a vendor isn't on panel? What happens then?

Davis: It is a great question, Ben, and it is something that we work diligently with our clients to make sure they're prepared for. There are different approaches by

different insurance carriers to how they manage their panels, their incident response vendor panels. Some of them are very flexible in the selection of a particular vendor giving an insured a lot of choice. Others are very inflexible.

So, usually the process, as long as we have preparation, it can go very smoothly. What we like to do is facilitate an initial informational interview with several privacy law firms, forensics vendors, sometimes a PR firm or notification vendor, and have our clients get to know the key individuals that would be working on their account. And then once they've made a selection after those interviews, we go to the carrier, and we disclose who they've chosen. For the most part, the carriers will want to know the negotiated hourly rates with that particular vendor if the client has a pre-existing relationship already. But usually with a little preparation, most carriers are pretty understanding and can add particular vendors to a pre-approved list.

Wanger: It sounds like it is really in the university or school's interest to really make their plan first, and then they can have exactly who they want on there instead of being shoehorned into certain vendors.

Davis: That is right, 100%. Now, there are certain products out in the market that really limit the scope of vendors that you can use, but we try to be very clear with our clients, hey, this is a very unique product. It is one of the reasons why maybe it is a cost-effective product, or you're getting certain additional features, but the compromise is you don't have that flexibility in the selection of privacy counsel, forensics, and other vendors.

Wanger: So, let's talk a little bit about the proactive side before a school ever has an incident. What resources do you see that are available to schools from their cyber insurance, especially ones that are being underused? How can schools best use those resources in preparing for the cyber incident response process?

Davis: Yeah, Ben, I would say that is where we've seen a lot of developments in the last, I would say, five years. There is a lot of competition in carriers offering very competitive risk management offerings. Our clients sometimes under, like you mentioned, underutilize those resources. But some of the ones that we find the most benefit to our clients include complimentary or discounted tabletop exercises. Sometimes those tabletop exercises can be tailored to a specific scenario or a specific industry class and that is always a fantastic idea. And it is a great way to get to know folks like yourself, Ben, privacy counsel, help them get familiar with your organization, your technology stack, your incident response plan, and it is a fantastic thing that carriers are offering.

Wanger: Yeah. I find myself, I do 10 or 15 tabletop exercises for universities a year, and they are totally invaluable. Just practicing that process, making sure that everybody knows what their role is, what other people's roles are. I find that at universities, given their structure, everyone doesn't know what everybody else is doing. So, I think that the ability to sit down and talk about who does what in the incident response process, it not only makes the university more comfortable that they are prepared, but it prevents hurt feelings and anger during the process

when people say they should have been involved, they don't understand why they weren't contacted. I agree with you. They're really valuable exercises in preparing.

Davis: And it really aligns with the mission of those clients as well. Collaboration, thirst for knowledge, it truly helps foster a collegial response, a coming together at a time of crisis, and if you can have an effective plan before you're actually in an incident, it is really invaluable.

Wanger: Tom, are there any other resources that are available to schools or any insureds with respect to cyber insurance that you see being underutilized?

O'Neill: Yeah, absolutely. And maybe the number one thing that I see underutilized, which is a true resource, is something that Paul had mentioned when we first started our conversation, which is the onboarding call. I think it is so important for clients to get to know their carrier, to get to know their policy, to get to know how their carrier expects them to behave in an incident response situation if they're filing a claim. So, that onboarding call is a great opportunity for our clients to get a download of all of those processes and feel confident that they know how to report an incident and how they're going to incorporate that data into their incident response plan. And that is just a simple 30-, 45-minute Teams call that you can do or a phone call. That is a great resource that pretty much any carrier should be able to provide.

In addition to that, like tabletops, many carriers are offering additional resources. Incident response plan reviews is one of my favorites. The incident response plan document should be a living, breathing document, something that you continuously evolve and it is pretty much on every CISO's list of things to do is to update that incident response plan. So, to the extent that you can use your carrier as a resource to the redlining exercise, I think is one of my favorite exercises to make it more of a usable, readable document. I think that is another great resource.

Wanger: Do certain cyber insurance carriers cover the costs associated with updating incident response plans?

O'Neill: They can, yeah. It may be at no cost, it may be at a reduced cost, but it is something that some carriers will do. So, definitely it is the type of thing you want to work with your broker to understand what resources your carrier provides. But yes, it can be at no cost or at a reduced cost. To a certain extent, like sometimes these resources depend upon the premiums that you pay. If there is a higher premium that the university is paying, that may open the doors for more resources to be provided at no cost. But it really depends on the carrier.

And in addition to that, I'll just add a couple more things. I've seen carriers offer certain privacy monitoring services. They may provide certain assessments of your Microsoft 365 environment, MFA-resistant keys, the Yubico keys, or some other kind of USB MFA key. So, it is all about understanding what is available to you when it comes to the carrier resources, because as Paul mentioned, there is

a bit of an arms race amongst the cyber insurance marketplace. Carriers are trying to develop more as they make their value proposition to the client better.

Davis: Yeah, Tom, I'd also add that we've been seeing a number of carriers, especially some of the newer entrants into the market, offer additional security offerings. So, extending beyond just a risk transfer product and providing things like managed detection and response services, so MDR services. So, they actually go in and will actually manage alerts and the triaging of your EDR solution. I would say as a broker advising a client, sometimes I'm a little skeptical having your insurance carrier also provide those security offerings, but it is an area where we're seeing a lot of growth and a lot of innovation.

O'Neill: Yeah, it is an interesting part of the equation, right? We've always been focused on the policy. Now we're focused on the resources. Now we're incorporating security into it, all coming from the carrier. And it just goes into that conversation with your client and their relationship with them. If those vulnerability assessment tools or those security scanning tools are valuable to you and you're utilizing them, then that changes a conversation about whether we are marketing your business to look for a different carrier.

Wanger: It is great stuff. So, the last issue I'd like to talk about with you guys is the cyber claims process. That is another issue, another process that really as the incident response counsel, I'm not a part of. What is your role in the claims process? How are you advocating for clients during that process?

Davis: Yeah. Ben, it is something that usually comes out in that onboarding meeting that Tom mentioned that we have with our clients. But we offer to all of our clients to help them report their claims to their insurance carriers, including their primary carrier and any excess carriers. We also step in and have an entire team within our organization that are former claims adjusters, attorneys that will actually step in and advocate on behalf of our clients if there is some sort of coverage dispute and they have regular communications with some of our largest carrier partners.

We also do things like the creation of business interruption worksheets that we share with our clients. So, it gives them an idea of what type of claims expenses may be covered by insurance so they can collect that data on the front end throughout the incident response process, rather than trying to scramble and put that together at the end of a claim. I think really just making sure that we have constant, or not constant, but effective communication with our clients throughout the entire incident response process.

Wanger: So, one thing that we do as the counsel representing our clients in incident response matters is we are in constant contact with the insurance carriers, basically making sure that they're available or they're aware of every penny that we're spending. We are giving them budget updates for legal, for other vendors. We're checking with them before ransom payments are made. We are keeping them in the loop throughout, making sure that they're on board and there is no objections to costs that are being incurred. One of the main reasons we do that is so that our clients are not having coverage disputes afterwards where the

insurance carrier is seeing certain expenses for the first time, and then there is a dispute over it.

So, Tom, what are some common coverage issues or disputes that you see in the education context on the back end of cyber incident response matters?

O'Neill: Yeah, sure. And for me, the first thing that comes to mind is, goes back to something that we were talking about previously with regards to panel vendors and using approved vendors. So, I think some of the biggest challenge that our university clients can face is if they do go off panel and their policy does require that they use panel vendors, that can be a situation where the carrier may decline to provide coverage for those bills. Or they may look at what the hourly rate was for a certain data recovery service that you purchased. And if those rates are deemed unnecessary or out of line with their requirements, those are things that they may only offer to pay for what their standard rates are. And really those are all avoidable issues, and it all comes down to collaboration and communication.

So, to Paul's point, that is why we spend a lot of time with our clients making sure that throughout the claims process, we are cc'd on all the emails and that we are in the loop of what the next steps are, so that we can help them avoid those pitfalls when they think about seeking a vendor that is not approved or is not on the panel. Those are things that we want to get pre-approval for before we end up in a situation where we're trying to recover a bill that we're not, that was not pre-approved.

Wanger: Paul, communication aside, is there anything that I can be doing or can my colleagues that we can be doing for our clients in the incident response process that will help them from a coverage perspective? Is there anything that we should be doing or could be doing more to help them?

Davis: I think it comes down to just avoiding those avoidable issues. For example, some things that we just generally know are going to be difficult to find coverage for. For example, we've had some clients try to claim the expenses associated with a salaried employe's time, and traditionally, that is not covered under a cyber insurance policy. Additionally, we've seen some insureds try to claim an incident response bonus payment to salaried employees as a covered element of their insurance policy and that, in general, is not covered. It would be really helpful if you start to see maybe a client disclosing that they're going down a certain path and trying to claim something that is traditionally not covered by a traditional cyber insurance policy, just helping them get back on track with the help of brokers like Tom and I, but I think that would also be helpful.

The final point, Ben, one of the other issues that we see that it commonly leads to some sort of coverage dispute is late reporting. And it is usually not an issue that you would encounter, Ben, because you're getting involved usually when the insurance carriers have already been put on notice. But we see many times our clients are, or clients maybe incur expenses or start responding to an incident before putting their carrier on notice. And that just leads to a whole host of issues

on the back end, not only trying to get those incurred expenses covered by the insurance carrier, but it is just very messy. So, I guess if you are interacting with one of your clients, it would be really helpful if you're asking questions about cyber insurance and inquiring about their policy and trying to make connections with the client's insurance broker.

Wanger: I think that really underscores the point is that we're all working together on this, the brokers, the attorneys, the other vendors. And I think the more we're in communication, the better we're servicing our clients.

Davis: Couldn't agree more. Yeah, and viewing everybody as a partner rather than taking an adversarial position. There is a time when you, when we do need to step in and advocate for our clients and take a position that is in direct conflict with an insurance carrier, but for the most part, everybody wants to have a successful resolution, and that is good for everybody's bottom line and reputation. So, viewing everyone, including your carrier, as a partner, I think is a good way to approach incident response.

O'Neill: I certainly agree with that. And when we have debrief calls with our clients about how their claims experience was, what the lessons are, the overwhelming amount of feedback that we get from clients and the different communications and the service that they receive from attorneys and other vendors, the overwhelming thing is appreciation. These are majorly disruptive events for our university clients. And the expertise and the value that the law firms and the forensics folks, the ransom negotiators, everyone really brings to the table is just so appreciated by the schools. It just makes it all the much better, again, when you lean into the collaboration, so.

Wanger: Well, it is nice to be appreciated. And I appreciate both of you joining me to talk about the broker's role in the incident response process, especially as it pertains to educational institutions as I know both of you are very active in that space. So, I thank you very much for taking some time to talk with me today. I look forward to working with you both to help our mutual education clients.

Davis: Thanks, Ben, and thanks, Tom.

O'Neill: Thanks, Ben for having us.

May: If you have any questions for Ben, his contact information is in the show notes. As always, thanks for listening to BakerHosts.