Podcast Transcript

Cyber Threats Facing the Gaming Industry and How to Protect Yourself

Date: December 12, 2024

Guest: Ben Wanger, Alexandra Bretschneider, Heath Renfrow, **Host:** Amy Kattman

Run Time: 21:28

For questions and comments contact:

Ben Wanger

Counsel
Philadelphia
T: 1.215.564.1601 | bwanger@bakerlaw.com

Kattman: On October 9, Counsel Ben Wanger attended the 2024 Global Gaming Expo in Las Vegas. Ben participated on the panel titled Lessons Learned One Year Post-MGM & Caesar's Cyber Attacks, alongside two other experts in cybersecurity and cyber risk management. Together, they discussed the threats facing entities in the gaming industry. I'm Amy Kattman, and you're listening to BakerHosts.

On today's episode, we'll hear from Ben Wanger, Alexandra Bretschneider, and Heath Renfrow. Ben Wanger is counsel and member of BakerHostetler's Digital Risk Advisory and Cybersecurity team. Alexandra Bretschneider founded and leads the Cyber Risk Management practice at Johnson Kendall Johnson. And Heath Renfrow is cofounder of Fenix24 and the Chief Information Security Officer at Conversant Group. Welcome to the show.

Heath, we are one year removed from the MGM and Caesars' cyber incidents. Could you give us background about those incidents and what really rocked the gaming industry?

Renfrow: Yes, ma'am. With Caesars and the MGM, there is a very sophisticated threat actor, and you can Google this, called Scattered Spider. Scattered Spider is a group of cyber criminals that are made up of basically teenagers, average 15 to 23 years old but they're extremely, highly technical. And in these situations, with Caesars and MGM, it was social engineering, but a very unique way of doing that.

This particular threat actor, over the course of a few years, had broken into most of the telecom industries' databases and taken phone numbers and names out of

it. In this situation, they targeted LinkedIn, found system administrators for both of these casinos, and then called the help desk for those casinos. And when you have these threat actors, English speaking, so they're U.S. and U.K. citizens. So, the social engineering was, I've locked out of my account, I need you to set my password. They verified, the help desk did, by sending SMS text message with a number in there to verify who the person was. Well, these threat actors had done a SIM swap, in these situations, and taken over the phone number for these system administrators. And they were able to sit there and verify that SMS code, and from there, they were able to gain access. When it is a system administrator, they have pretty much God privileges inside most clients' environments. And so, this threat actor got access and then they moved through their cloud environment, their on-prem environment, and really took and caused a lot of chaos across the board, in both those situations, within a week time frame.

And it really caused a lot of damage in the gaming community and really rocked the world. The whole world was focused on that, especially with MGM actually suffering the encryption process. With Caesars, Caesars actually reached out proactively to the client because Scattered Spider was active in their environment and started negotiating a ransom to be able to sit there and get them to leave them alone. So, MGM did not take that route, unfortunately. It did get encrypted and the rebuild and recovery process took roughly about 10 days.

Kattman: Ben, have we seen a change in practices in the gaming industry following the MGM/Caesars incidents?

Wanger: So, I think we have on one hand. And on the other hand, we really haven't. I think a lot of the large entities, especially MGM and Caesars, have taken a lot of precautions and invested a lot of time and energy following that incident in their security practices, in making their systems more secure, in making sure that they are prepared for an incident in the future. And that, to the extent that they have an incident in the future, again, they have preparations in place so that they can minimize the business interruption.

That said, I think a lot of the smaller-end gaming entities, probably they saw what happened to MGM and Caesars. There was a lot of, well, that couldn't happen to us, for them. So, I think, to a large degree, the practices in the immediate aftermath, you may have seen a lot of companies investing in cybersecurity and taking some actions to protect themselves. But I think as we get farther and farther away, a lot of the other entities have not changed their practices much from what they were before, and there are still areas where they can improve their cyber security posture.

Bretschneider: To your point, Ben, it is a blessing and a curse. So, in the one hand, you've got an entire industry that witnessed these major incidents for both MGM and Caesars and the impacts from the casino floor to the hotels, etc. And so, I think that opened eyes to say, wow, we are also an industry that could be targeted and impacted. But to your point, I think the curse side of it is it still left that impression of, well, yeah, it is because the bad guys go after the big guys. As opposed to, no, it is actually size and, frankly, industry agnostic who could be targeted. There

is still a little bit of a perception that I see out there of, it is not going to happen to me. And, Heath, please chime in.

Renfrow: No, you're exactly right. The news right now, over the last five days, you'll see a major gaming institution that's been hit by ransomware event. But we have done 30 casinos since MGM, Las Vegas or Nevada _____. But a lot of tribal casinos, a lot of casinos in Canada, they are very, very much still a target. And it is a hot target because you think about how much revenue is affected in these situations.

But also, customer care. A lot of these casinos, regional casinos, that they depend on their regular customers. Unlike Las Vegas, who might get the same customer once or twice a year. These regional consumers, their consumers come in two or three times a week. And when you're down, and you cannot sit there and provide your perks to them, they cannot gamble. They end up going to other regional locations to be able to sit there and enjoy what they do and to be able to gamble and get the benefits of it.

So, the impact, really, is far-reaching for a lot of these casinos. And they're actively being attacked. It doesn't matter, and I haven't truly seen a change in the security posture in most organizations we've seen. It is short-term memory, is the best way I describe it. It can't happen to us, MGM and Caesars was one-off. We don't have the money to invest in this. It'll never happen to us. And then wham, bam, it happens. Historically, from my experience, the gaming community is extremely behind. I put it on the same level as healthcare when it comes to security and the technology and investment they put into it.

Wanger: Yeah. And, Heath, one thing I'll add to that, on what you said, is in talking to clients in the gaming industry, one of the things, the risks that they have when they have these incidents, are they have a lot of competitors. So, if their customers get a negative opinion of them, if their customers can't go to the hotel or gamble on a certain day, they have a lot of other options. And once they start going to another casino or staying in another hotel, well, they might enjoy that more and then all of a sudden, these gaming entities have lost a customer. So, I think that is a real big risk for them when they're having these incidents as well.

Kattman: Ben, what would you say are the biggest cyber threats facing entities in the gaming industry?

Wanger: So, I think that the cyber threats that are facing these entities are similar to the threats that you see all industries face. The two biggest ways that these threat actors are getting into networks are social engineering, which is what Heath talked about with Scattered Spider – sometimes it is e-mail, sometimes it is over the phone – and unpatched vulnerabilities in their network.

And these vectors are leading to the two largest types of incidents that we see are network intrusions, which lead to ransomware. Often where these threat actors somehow get into the network and get access, and then either encrypt systems or steal data. And then the other is e-mail compromises, where these

threat actors will try to get into the e-mail of somebody at the casino who is in charge of payments, and they'll work to redirect a wire transfer. So, whether it is a vendor of the casino or the casino itself thinks they're making a payment to a legitimate entity, but they're actually paying that money to threat actor.

Bretschneider: I would love to add a couple of thoughts here. So, I think the way you ask the question, Amy, is interesting. Right? You said, what are the biggest cyber threats? And so much of what Ben covered are the ways that organizations are being targeted, but I would even take it a step further. When you think about the threats to the business, right, it is also what are the impacts. And I think what we saw with MGM and Caesars and what we experienced with other similar organizations, whether they are land-based casinos, online gaming platforms, etc., is that the impacts can certainly be operational on their ability to provide the services they were providing before.

Compliance and regulatory, right? So, when an incident involves a breach of personal information, you now have a host of compliance considerations and regulatory considerations that you need to work through in order to potentially resolve the incident in accordance with law. You've contract requirements, of course, and whatever obligations you have to notify suppliers, vendors, etc.

And then, of course, financial. Right? All of these things impact your bottom line. And I think, Ben, you made such a great point on the last question around the loss of a customer. Right? This can transcend beyond impacting you only while the incident is in effect. But the future prospectus of your organization in terms of, alright, if we lose X number of customers because they can't bet on this mobile app and therefore, they open up another one because they want to get their bet in before the game goes off. That is pretty extraordinary in terms of when these organizations have to look at the cost of customer acquisition versus attrition. And so, I think the threats are far and wide and very impactful to these types of organizations.

Kattman: Alex, what can entities in the gaming industry do to mitigate those threats and/or the impact of those threats?

Bretschneider: Yeah. So, when I think about cyber risk management, and if you're listening and you are not someone who considers themselves remarkably tech-savvy by any means, I think we can break this down into very logical parts, right? Cyber risk management is a combination of people, process, and technology. And I think when we hear cyber, our minds automatically go to technology and that is where we focus. And there are very important technology-based measures you should take, right? Having multi-factor authentication on remote access and e-mail access to prevent an outsider from hopefully getting in. But that is not a panacea, right? That doesn't prevent everything from happening because we get MFA fatigue, and we still let the bad guys in.

So, that puts us back, then, focusing on the people and process side of the equation. So many of these incidents, as Heath described, in terms of what actually happened with the social engineering, that was people and process

focused. Right? Training people to be skeptical and creating a culture where skepticism is really welcome within an organization that that is not considered rude. We raised a generation of people pleasers, that now it feels uncomfortable to question the authenticity of something when really that is, unfortunately, what we need to be doing.

Beyond that, the reality is this. There is no such thing as reaching a state of being what is considered cyber secure. There is no certification you can get. There is no compliance framework that unequivocally says, you can go to bed at night and say, yes, I did it, I'm cyber secure. So instead, the focus is on being cyber resilient, right? In creating processes and people and technologies that allow you to sustain an incident and survive it and persevere.

And one really important component of that, of course, and this is a shameless plug for my industry, is the insurance side, right? Nobody is allocating dollars on their balance sheet right now for if and when they have a cyber incident. Instead, you're better served considering the risk transfer mechanism that insurance affords. So, all the types of things that go into resolving the incident, whether it is legal counsel from someone like Ben, restoration services from somebody like Heath, notification if that was required to individuals that were breached, paying a potential ransom, lost profit to your business, all of those are actually intended to be covered by a cyber insurance policy. So, in terms of protecting your balance sheet and making sure you have the ability to be financially resilient to an incident, cyber insurance has to be part of that equation as well.

Wanger: Just to add to that, I think it is great that companies are doing all they can to protect themselves from a cyber incident, education, investing in defenses. As Alexandra said, I think one of the most important things to do is accept the fact that you can't be completely secure. So, make sure that you know what to do when you have an incident. And practicing that and making sure that you spell it out in advance is extremely important. The last thing you want to be doing in the middle of an incident is figuring out who is in charge and what do you do. So, whether it is doing tabletop exercises where you practice the incident response process, making an incident response plan and evaluating that plan regularly to see if you need to make any changes, those are things that gaming entities, and really, any entity, can do that can really greatly mitigate the impact of an incident if and when it happens.

Bretschneider: Yeah. The only thing I wanted to add is just when you have a cyber insurance policy, insurance is a reactionary measure. It is meant to help you at time of incident. So do not be shy to tap into it and use it, and it is going to bring the most experienced folks in the world to your side. So, the folks like Ben, like Heath, who live these types of incidents all day, every day, that is all intended to be brought together as part of your coverage. You don't have to go out and find these folks, they're availed to you as part of having that policy in place.

Renfrow: Yeah. I'd love to chime on from the technology side since we have recovered clients. I've been doing cybersecurity a long time, risk management is extremely important. It takes a lot of buy-in from executives. It is hard to sit there and do

risk management if you don't know what your critical assets are and the order of that. It goes back to Ben, also, from an incident response standpoint. Almost every client we've ever had, Fortune 50, 500,000 casinos, it doesn't really matter. They don't understand their assets and they don't understand their order of operations to recover those assets. A tabletop exercise is great, but if it is just pen and paper, it doesn't really prove whether or not you can recover from your backups, and that is where I focus.

The number one cybersecurity control, in my professional opinion, and this is somebody that's run global cybersecurity programs in the past, is backups. Immutable, tested, valid backups that you can recover from. So that is just the truth. You got to be able to sit there and be able to recover, and most clients don't. Their backups are usually gone 95% of the time. And when they're not gone, they just don't understand their assets. They don't understand what to recover first and that is what drives up business interruption costs. And so, backups, backups, backups. That is where I'm at. Risk management is fantastic, understand your critical assets, do the tabletop exercise. But backups are always assumed that they will be there. They're an afterthought. But I, in even an afterthought in my past life, I just assumed they'd be there. They're not. They're not, they do not survive. These threat actors work very hard to cripple your backups. They want you to have to pay them. So, they're going to make it very difficult on you to recover.

Wanger: And just to add to that, one other point is, one other thing that I talk to clients about a lot, and I think is a really good exercise is for companies, is to think about, what are your crown jewels? What is the most important data that you have? So, I think knowing that, first of all, if you think about that in advance, you can make extra efforts to protect that data. But then, in the event that you have an incident, knowing what data you need to know right away if that was involved, I think can really expedite the incident response process and help you make some of those hard decisions, like is there a need to pay a ransom? What kind of notification obligations are we going to have? So, I think thinking about things like that in advance really help on the back end.

Kattman: Ben, in the event of a cyber incident, what are some of the key considerations for entities in the gaming industry?

Wanger: So, there are a lot of considerations that an entity has to go through when they have a cyber incident, such as figuring out exactly what is affected, what vendors they want to engage. The one that I think is under-discussed, and really the difference between a small incident often times and a large incident, is communications. How the entity is going to communicate about the incident is often the difference between what the public perception is going to be. If you communicate in a way that shows you know what you're doing, you're not saying things that are going to make people nervous, you're showing that you are trustworthy, I think that can go a long way in minimizing the negative impacts. So, I would advise entities in the gaming industry to think about their communication plan in advance. Because in the event of an incident, you want to make sure that

you're being consistent and you're communicating about the incident in a way that is not going to make this larger than you want it to be.

At the same time, there are also several legal considerations. You want to make sure that you are keeping the regulators involved and up to speed. You want to make sure that you are assessing what your notice obligations are. And you want to make sure that you're complying with those obligations because, again, casinos are very highly regulated, and it is very important to make sure that you are meeting all those obligations. Because, again, there could be penalties if not.

Kattman: So, as we closeout today's program, I'd like to hear from each of you what you learned from the Global Gaming Expo conference. It would be helpful in providing assistance to companies in the gaming industry. Heath, let's hear from you.

Renfrow: It certainly looks like new technology is being brought in all the time into the gaming industry and they're looking to advance. So, you look at that, you're looking at different providers that are going to provide that. So, the thing I've learned and look at now is not just on-prem data being taken down, and you have that similar incident right now going on in the United States where a provider that provides law services across the entire industry has been affected, which Cistern causes a lot of issues. It is similar to what you saw in the car dealership industry a couple months ago, with their major provider that provided a ton of services being down. And it significantly impacted the car industry because they weren't able to process that.

So, something I've seen in the casino industry is a supply chain risk when they're leading other vendors to be able to bring their platforms in, should it be an app that Cistern allows clients and vendors to be able to sit there and log in and book their rooms or track their casino betting, those type of impacts across the board can really impact the whole industry. So, security, from that perspective, is not just internal to the gaming industry, but also the vendors that provide services.

Bretschneider: I'll jump in here and say what I learned was we had, if not the highest, one of the highest-attended breakout sessions of all the sessions held at the Global Gaming Expo. Which tells me that the industry does know they need to care. But then based upon the participation, the questions we got, and then obviously our experience of seeing ongoing incidents within this industry, they're still woefully unprepared. So, I think they know they need to start thinking about it, that it is something that is real and present. But I think they're still miles to go in terms of improving their cybersecurity posture.

Wanger: I had a similar observation, is that one of my observations was, is that there definitely, in the gaming industry is, there is a feeling of investment in cybersecurity defenses and an understanding that this is a real threat. But I felt like there was not a great understanding of the incident response process. There is a lot of understanding of what we have to do to protect ourselves, but not as much of what we do if and when an incident actually occurs. And that is why I have underscored the importance of doing tabletops, making sure that you have

an incident response plan. Because I think that is almost as important as preventing an incident, is being prepared for how you're going to react if and when an incident occurs.

Kattman: Ben, Alexandra, and Heath, thanks so much for this informative discussion today. If you have any questions for Ben Wanger, his contact information is in the show notes. As always, thanks for listening to BakerHosts.