CARLTON FIELDS

Canna We Talk Cannabis? Cybersecurity Risks Bring Growing Pains to Cannabis Businesses

February 10, 2020

This episode explores the circumstances involved in a recent data breach involving the cannabis industry. We explore cybersecurity and data privacy issues that all cannabis companies need to

consider, and provide practical cybersecurity tips that cannabis companies should consider to better protect their business.

Transcript:

Kevin McCoy: Hello everybody we're back for another episode on the Can We Talk Cannabis podcast. I'm Kevin McCoy at Carlton Fields. I'm in our Tampa office and the co-chair of the National Cannabis Taskforce. I had an opportunity recently; I was talking with the practice group leader for our Cybersecurity and Privacy Group, Joe Swanson. We were talking about some new issues that are emerging in the cannabis and the crossover between our two practices as we see this new technology, if you will, in cannabis go mainstream and more and more businesses who are experiencing some of the more routine problems that are coming across for those who are handling any kind of customer data. So without further ado, I'm going to introduce Joe Swanson. Joe, thanks for joining me today.

Joe Swanson: Thanks, Kevin. It's good to be here.

Kevin McCoy: Joe, maybe give the audience a little bit of your background on the cyber side and what you do here at the firm.

Joe Swanson: Sure, thanks. So, I am a shareholder in Tampa with Kevin. I oversee the firm's Privacy and Cybersecurity Practice Group which has practitioners in a number of our offices throughout the country. And a number of us, including myself, were formerly federal prosecutors who handled cyber investigations and prosecutions. So, we have tried to apply what we've learned in those experiences to the benefit of our clients on the cybersecurity and privacy side. And, I am excited to be here talking about this for you and your clients.

Kevin McCoy: So, Joe when you talk about applying some of the things you learned as a prosecutor, I supposed there you were mostly dealing with after-the-fact issues and trying to prosecute criminals who were breaching systems and bringing them to justice. But, here your practice on the civil side is both preventative for businesses and reactive. Is that fair?

Joe Swanson: It is. Yes, we break our practice down into a few different buckets. The first being the preventative work like you talked about: drafting the policies and procedures, incident response guides, which are something I'll talk about a little later this afternoon, and other kind of peace-time activities that companies should be doing to mitigate their risk from cybersecurity incidents and breaches. The other bucket that we deal with is the flip side of that which is breach response. And then the third bucket is litigation associated with those events, which unfortunately is increasingly, sort of common event once there is a significant breach or other incident.

Kevin McCoy: Let's talk about litigation, because that's really what got us together as we were chatting recently. And, as I understand it, one of the main events that happened recently is that there was a data breach that has now targeted the cannabis industry. Even though this is an emerging industry and one that's growing rapidly across the country. They are not immune already at this growth phase to being a target of those who are wanting to steal some data.

And as I understand it, we had a dispensary and obviously they are gathering a large amount of data from customers, from patients, both personal and purchase information like credit cards, things like that. But, tell us what happened in this particular case, and we'll walk through it and give some practical tips to those who are listening and maybe needing some of that preventative counsel that you give.

Joe Swanson: Sure. So, what happened here was, there was a data breach involving a cannabis software provider named THSuite. And, THSuite provides a variety of services to its clients and among them are point-of-sale and inventory management for cannabis companies. Those are their clients. And, in this instance, THSuite, as many companies do regardless of cannabis industry or not, used a cloud service provider and it appears to be Amazon web services here, which is one of the biggest. And, by virtue of the way the data was stored in the cloud, allegedly there was a vulnerability there and it was exploited. And, that exploitation of that vulnerability led to a data breach involving at least three of THSuite's customers. Those three customers being dispensaries. And so, the breach involved information that belonged to those dispensaries and was being managed or stored for one reason or another by THSuite. And, the information at issue, at least as has been reported so far, really runs the gamut of the kinds of things, it's a great illustration of the risks associated with data breaches and points out a lot of things that tend to get overlooked. So, the information here involved PII, Personally Identifying Information.

Kevin McCoy: And what are some examples of that, Joe?

Joe Swanson: That could be, you know, in most states that's name, social security, name and health information. Health information can come into play here because you've got patients possibly who are visiting the dispensaries whose information was being stored by THSuite. So, you may have patient information which raises some HIPAA concerns, which I'll get to in just a moment. And, then you have more garden variety PII: name, email address, phone number. That's not always a PII, depending on the jurisdiction you're in, but it can be and if nothing else it can cause issues from a customer relations standpoint.

Kevin McCoy: So, Joe, in terms of this being a unique fact pattern to cannabis, this strikes me as something that's kind of similar to what we've seen in some more classic data breaches with big retailers and big box stores where it's not really the store, you know, say Target for example, that is

the target. The vehicle to get in is actually through some of their other contractors that they are using for ancillary services. Is that right?

Joe Swanson: Yeah, that's absolutely right. And that is why vendor management is such an important aspect for cybersecurity preparedness and due diligence when you're selecting your vendors, because, as you say, they are often the weak link that is used to carry out one of these attacks. As you pointed out in Target, the means by which the attackers got on to Target's system was through an HVAC vendor in western Pennsylvania. Nobody remembers them; they remember Target. And so from a PR standpoint, the vendor tends to get forgotten and it is the public facing company that has the PR and other issues associated with it.

One other thing about the nature of the information here. It was in addition to PII, sensitive business information. And that often gets overlooked because everybody is concerned when there is a data breach, understandably, with what their notification obligations might be to their customers or in some cases their employees. What they tend to forget is that there also may be sensitive business information.

Kevin McCoy: Trade secrets.

Joe Swanson: Trade secrets, customer lists, sales information. It looks here like these three dispensaries had inventory information, employee information that was compromised as a result of this incident. And that can raise some, you know, difficult questions about the relationship going forward between THSuite and the companies that it serves. What do the contracts say about liability and indemnification in that kind of a situation? So, you know, one thing that people need to be cognizant of when it comes to cybersecurity is it's not just about securing PII. It is also sensitive business information that could really be a competitive issue were that to get out.

Kevin McCoy: Yeah, you know, that's a good point. I have written on some of the prior blog posts about the sensitivities of trade secret information in the cannabis space, because at the federal level there are still some very serious challenges in terms of other IP protections that you can get because of the federal stance on cannabis in general, particularly any kind of product that is associated with the marijuana side of cannabis as opposed to, you know, say example CBD. But trade secrets become even more important. I mean, everybody who has a trade secret thinks that that's the most important secret in the world and sometimes it is, but here where you can't get other forms of protection that is certainly something to keep an eye on in these types of scenarios because that's the crown jewel, whether it's a manufacturing process, it's something that's giving you that competitive edge against those who are trying to get into this emerging industry. So I appreciate you pointing that out.

Joe Swanson: Sure.

Kevin McCoy: So what was another feature? You mentioned here "the cloud" and just help those who are not acquainted with that aspect of this particular case understand what was going on and how the cloud came into play.

Joe Swanson: So the cloud came into play here because it looks like THSuite, like, you know, companies around the country and around the world for that matter are using cloud storage for some, if not all of their data storage needs. So the cloud storage where you pay a company like AWS or another entity to store your data for you, it's not actually stored onsite. If it's stored onsite it's on premise or on prim and, you know, probably be on servers that the company purchased. Going to the cloud has certain efficiencies. You don't need to buy all of that infrastructure and maintain it. You know, if you go with a big company the idea is that you're also getting their security, you know, that comes along with the fact that they are maintaining data for tens of thousands of customers.

But, as companies move to the cloud they need to be cognizant that these types of events can happen and the hackers know that there is a wealth of information in the cloud. And often no matter how robust the security is with a Native US or other major cloud service provider, the way in which the storage space is set up for that particular client there may be some vulnerability in the way that it was setup as it appears may be the case here. And so all the security in the world doesn't matter if there's some problem with how that database was arranged. And, you know, then the issue is going to be, among others, who bears the responsibility? Is that going to be Amazon's problem? Is it going to be Amazon's customer's problem, which is THSuite? And so there the contracts also becomes critical. What is the apportionment of risks between THSuite and Amazon web services? I have a feeling it is very strong in favor of AWS just given their power in the market place.

But as people look to go to the cloud, particularly in this space, they need to look at what those cloud service agreements say about security. Are there reps and warranties about security? What kind of indemnification is there if there's a problem? If there is a breach who's going to give notice, the cloud service provider or the customer? All of those things will get sorted out in this instance.

Kevin McCoy: And how often are you getting called to engage in those kinds of analyses for clients that are coming across and we are servicing or are entering, whether its cannabis or anything else? I mean, it seems to me that that's not only a big negotiation point but a point that deserves attention in the finer details.

Joe Swanson: Yeah. It comes up all the time, whether it's in the cannabis industry or otherwise. Again, because of the premium placed on vendor management as a cybersecurity risk to be considered, you know, we are working with clients increasingly on what those contracts say about allocation of risk, reps and warranties. If there's cyber insurance, is the contract counter-party named as an additional insured under the cloud service provider policy?

Kevin McCoy: Yeah, yeah.

Joe Swanson: All of those things come into play just as they will in this case.

Kevin McCoy: Let's talk about just the focus on security and if you had some takeaways here and tips for those who are listening as just the practical pointers. Because as you're seeing this market emerge as cannabis is becoming a mature industry expected to generate billions of dollars whether you're in a medicinal or a non-medicinal or recreational or non-recreational state you've still got the entire CBD industry. And so, all of them are starting to come into a posture where they're handling data, whether it's point of sale, whether it's customer, private information, especially on the medicinal side, on the marijuana side. You mentioned the HIPPA laws and protecting health information just like you would the expectation that you have going to any doctor that your information won't be made available to third parties or sold on the black web. So, what are the takeaways for those who are getting into the space or maybe are in the space but until now have really never given this part of their business attention?

Joe Swanson: Yeah, let's talk first about what the risks are which I think will underscore how important it is and you touched on a few of them just there Kevin. One is, if they're handling patient data and they are a covered entity which is a legal analysis unto itself, under HIPPA they may be subject to the HIPPA laws regarding cybersecurity and privacy. And there are a host of obligations with regard to maintaining the security and confidentiality of patient data. And where there is a compromise under HIPPA there are notification obligations to HHS. There are notification obligations to the patients. And there are a host of penalties that may come into play where there's non-compliance. That would be in addition to the garden variety breach notification statues that exist now in all 50 states that require notice to affected individuals whether it's employees - everybody forgets about their employees, but their employees' data can be compromised - or customers. And there may be notification obligations that kick in as early as 30 days upon becoming aware of an incident. And the notice would run to the individuals as well as to the attorneys general and other regulators, which could be a sensitive issue, I think, for some of the companies in this space.

Kevin McCoy: And you're talking about mandatory notification?

Joe Swanson: Mandatory.

Kevin McCoy: So this is self-tell.

Joe Swanson: It is mandatory and in some jurisdictions it's not just the attorney general but it's also the division of state police. So, you know, for companies operating in this space too where the, you know, legality of it is so jurisdiction-specific, that's another aspect to keep in mind to say nothing of

the private plaintiff's bar. You know, increasingly where there is a major breach you will see a major plaintiff firm if not more filing lawsuits, potential class actions within days of the incident being announced. Just the way that stock drop suits use to be filed when a stock slipped on the stock exchange. So those are risks that come at these companies from a variety of angles.

So in light of those risks, what can be done? You know, you pointed out, Kevin, that a lot of the companies in this space are growing very rapidly. And that's great for them and for those who work for them. The issue is often that growth is not accompanied by a maturity in controls that would help to reduce some of these risks. So these companies are so focused on growth and expansion that they can forget to have in place some of the policies and procedures and other documentation that would help them in the event of an incident. So what am I talking about there? Well, one of those is a written information security plan or program or a WISP. In some states like in Massachusetts if you do business there you must have in place a WISP, which is your written explanation for how your organization maintains and secures its information, everything from hard copy documents to electronic data. Most companies are not aware of that obligation and it can trip them up. So have a WISP in place. Another thing to have in place is an incident response plan, which is ideally very short accessible and usable document that sets out for the organization who's on the incident response team if there is a breach? How is it going to be investigated? What are the triage levels? When is law enforcement called? Kind of all the things written down so that if there is an incident there's something to turn to and people aren't just, you know, flying by the seat of their pants.

Kevin McCoy: Yeah, so let's talk about the incident response plan because I know what that is just from the kind of war games that we've been through here in the firm of better understanding this but it's the kind of situation where you have a plan and there's been a breach. It's been identified or brought to management's attention. And then we like to play the game well, the chief executive is now unavailable, on a cruise somewhere for the next 48 hours. But, that's when all of the stuff starts to happen where you have to start investigating. You may get ransom threats to expose the data. Help us understand a little bit more about how that sometimes plays out.

Joe Swanson: Yeah, again the incident response plan, you don't want it to be a lengthy document. You want it to be something that people know where it is, and you've practiced with it before. And, so, if there is an incident, you pull it off the shelf and you say OK assemble the six people who are on this team. And, yes, if one of them is on vacation or sick or otherwise unreachable, who is their back up? All of that should be spelled out in the plan, even with people's cell phone numbers and ways to get in touch with them on weekends and evenings, which is invariably when these things tend to happen. So have that incident response plan in place.

And whether it's that or just cybersecurity preparation in general, we like to tell our clients, particularly clients here in growth mode, don't let the perfect be the enemy of the good. Having something, and ideally something that you can follow, is better than nothing. So rather than sort of

throw up your hands and be paralyzed be indecision and, "Well, geez. We're never going to be able to put all of this together," just start somewhere. And a lot of these resources, a WISP, an incident response guide, you can find examples on the web. Get them, tailor them to your organization, know where they are, socialize them within the company, and then practice with them. And that will go a long way to reducing your risk profile because the studies are unanimous in finding that the sooner you can identify and contain a breach, your costs of responding go down dramatically. And so that's just critical. And if you are ever subject to regulatory scrutiny having these controls in place will be great things to point to, to try to mitigate your exposure with the regulators.

Couple of other points to mention when we're talking about tips and that is encrypting your data. The reports that I've read about this incident indicate that the data was unencrypted. Having data encrypted is absolutely essential where it's sensitive data and that's for a number of reasons. One, your contracts may require that you keep the data encrypted when it's on your systems or sometimes it's referred to "at rest". There may also be obligations in your contracts that it be encrypted when it's in transit, being sent from one place to another. Having encryption is critical not only to fulfill whatever obligations you have in your contracts, but also most breach notifications statutes have a carve out where there is no obligation to make the notice where the data is encrypted and thus unusable.

Kevin McCoy: Can you just briefly give everybody an understanding of what it means to have it encrypted for those who just aren't familiar with that process or what's go on there?

Joe Swanson: Yeah. I mean, encryption is a way of rendering the data unreadable and unusable without having access to the encryption key. And so, so long as the data is encrypted and the attacker has not also gotten his or her hands on the encryption key, in most states, you're not going to have to make the notification that everybody loathes and that is very costly and, you know, can really drive up the price tag on these incidents.

One final tip to consider and that is, there is increasingly a robust market for cyber insurance. And as these companies are growing and considering risk management and looking to develop insurance programs for a variety of risks they should, as well as their brokers, think carefully about whether they can get some kind of cyber insurance to mitigate these risks. That can be absolutely essential in keeping the costs down. And also having a cyber insurance policy typically gives the insured access to a panel of preselected forensic service providers, law firms, other third parties that you may call upon in a breach who've been vetted and approved by the carrier ahead of time and who tend to have negotiated rates. And so that's just another reason to really look seriously at cyber insurance.

Kevin McCoy: That's great. I think this is a fantastic overview and a way to get those who are not familiar with the risks of handling all of this data a little further down the road and at least thinking about this as a part of their business and something that is important and has to be addressed and

protected in various ways. So I really appreciate you taking the time today, Joe. This has been helpful. You can follow more of our content at Carltonfields.com (at *Canna We Talk Cannbis?*). And if you also have the ability, you can follow Joe and his team over at the Cybersecurity podcast. Joe, give a plug for the full name of that production that you all have going there.

Joe Swanson: Yeah. It's CF On Cyber where we host podcasts just like this one, talk about timely topics of interest to our clients. And we also maintain a Cyber APP which has a number of resources that the listeners may find useful, whether it's checklists and other guides to help them get into place the things we've been talking about today.

Kevin McCoy: Thanks a lot. We appreciate you stopping in over on the Cannabis Channel today and that'll do it for this episode. Thanks.

Presented By

Kevin P. McCoy

Related Practices

Cannabis Law
Cybersecurity and Privacy