Podcast Transcript

2022 DSIR Deeper Dive: Vendor Incidents

Date: June 29, 2022

Guest: Lynn Sessions and Stefanie Ferrari **Host:** Amy Kattman

Run Time: 18:12

For questions and comments contact:

Lynn Sessions

Partner
Houston
T: 1.713.646.1352 | lsessions@bakerlaw.com

Stefanie Ferrari

Associate
Chicago
T: 1.312.416.6229 | sferrari@bakerlaw.com

Kattman: Ransomware, MFA, extortion, fraudulent fund transfer schemes, these topics and many others make up the key finding section of the Eighth Annual Data Security Incident Response Report, informally known as the DSIR Report. Each year, the incident response attorneys within the Digital Assets and Data Management Group, or DADM, provides statistics and analytics around the incidents they encountered the previous year in a report that is eagerly received by clients, vendors, media outlets, and frankly anyone interested in or tasked with their company's digital asset and risks. I'm Amy Kattman and you're listening to BakerHosts.

This, our second episode in the series exploring the 2022 DSIR Report, discusses the surge in vendor incidents, along with lessons learned and ways to defend yourself from this type of incident. Our guests today are Lynn Sessions, partner and leader of the Healthcare, Privacy and Compliance team, and Stefanie Ferrari, an associate on the Healthcare, Privacy and Compliance team. Welcome to the show Lynn and Stefanie.

Ferrari: Happy to be here.

Sessions: Yeah, thanks for having us.

Kattman: Stefanie, I'd like to begin with you. So, we know vendor incidents continued to surge in 2021. What are the main causes behind these incidents and why are vendors such a high value target for threat actors?

Ferrari: Yeah, they certainly did continue to surge in 2021. Almost 20% of the total incidences we handled last year involved vendor causes, and more than half required notification. And the main causes we see with vendor incidents are consistent with other matters we handle and include things like phishing schemes or inadvertent disclosures, but the primary cause has really been ransomware.

So, this would be where the vendor systems are encrypted by the ransomware and can involve theft or access to customer data that is stored on the vendor systems or even spread of the ransomware to the customer systems. And that is part of what makes vendors these high value targets for threat actors, because they're storing a large amount of sensitive customer data on their systems or they have access to multiple customer environments, for example, like a managed service provider. And the threat actors can leverage that added pressure from customers for extorting payments from the vendor, particularly in healthcare matters. Lynn, do you agree?

Sessions: Definitely. We can see looking at the data from this year's DSIR Report, looking back on our 2021 incidents, that there was that added pressure, particularly in healthcare. In fact, we had at least one incident where not only was the vendor extorted, but the downstream customers were also extorted by the threat actor so that they could get back up and running from an operational perspective. So, when you've got the managed service providers affecting the day-to-day operations, or really any vendor that has that kind of impact on a customer's operations, you see that pressure come from the threat actor from any type of ransomware attack that may occur.

And large field vendors in the healthcare space, they work with multiples of healthcare entities across the country, and so if there is a ransomware attack or some other type of intrusion into their systems, that impacts a large number of healthcare systems across the country, then you see a significant impact not only to that particular vendor, but all of their downstream customers. And in the healthcare context, it could mean the difference between life and death, and then on the HIPAA front, because there is such a low threshold for notification, we have to overcome a presumption of a breach once its red actor has accessed

systems or has encrypted systems, then we do see that over half of the vendor incidents that happened last year resulted in some type of notification on behalf of those healthcare providers.

So, we are seeing a lot of notifications based on the data from last year's incidents, a lot of notifications coming out of the vendor incidents that can impact our clients, as we'll talk about later on in the podcast.

Kattman: What kinds of unique challenges do vendor incidents present to their customers? Lynn, let us begin with you.

Sessions: Sure, so the vendors have to communicate with their customers about the incident and some of that may impact the timing of when that communication takes place, the content of the communication that goes to the customers, and what the customers then do with that information. So, because there could be an impact to operations, the customers or our clients in many instances are having to make a determination on what it is that they need to communicate to their own customers.

So, because the impact on operations coming from the vendor, there could be additional communications that need to go out to, whether it is the media, to the customers themselves, to their employees, et cetera, as part of the notification. As we talked about complying with deadlines, that is when the vendor has to be very thoughtful about what it is that they would communicate with their customers, because when they put their customer on notice, there may be notification deadlines that then get triggered to those customers such that their breach notification obligations start at that point in time.

So, the customers are oftentimes at the mercy of their vendors, whether it is the information they get from the investigation, the amount of information they're able to get through the investigation. Of course, many of the vendors are, as we say, lawyer up, such that their lawyers are telling them not to share intimate information about the particular incident, and that can make it very difficult for the customer to make a determination on whether or not they need to notify. So, you find yourself kind of in that position of just consistently asking for more information, because we handle a number of these incidents, both on behalf of vendors as well as customers.

We get to a point that we can kind of read between the lines as to what the law firms and what the forensic firms are really trying to say, such that we can best advise our clients. Stefanie, anything you want to add to that?

Ferrari: Yeah, I think that is a really good point, and for a lot of our clients, particularly in healthcare, where they have their own really good incident response procedures, it can be difficult to kind of, like you said, them being the mercy of the vendor when an incident happens, because they're under their own regulatory deadlines like you mentioned, and based on their own incident response procedures there, they might be used to more level of detail coming in from forensics. But I think

that is a good point you made, that we can sort of start reading between the lines and seeing based on what they're saying. What do they really mean?

Kattman: Stefanie, can you tell us a little bit about the lessons learned in regard to these vendor incidents? What key findings stick out to you?

Ferrari: Yeah, so like we were just talking about in vendor instances, customers are really at the mercy of their vendors. So, one of the key findings that sticks out to me is the timing and the level of information that is shared by the vendor can vary a lot based on the vendor, depending on the type of incident it is or the nature of the services that the vendor provides. So for example, in a ransomware incident, the incident is pretty apparent to the customers right away because of that operational impact we talked about.

So, the vendor might rush to get out a communication to their customers and it could be incomplete or inaccurate, and then later on they are needing to clawback that information and correct it so that their customers can complete their notification analysis. And this can cause customers to have to repeat or expand their assessment as the investigation develops, and it can take a long time to get those additional details that the customers need to complete their analysis and determine what data was impacted and the customers that were actually affected by the incident, which leaves customers in a sort of holding pattern while all that gets sorted out.

So on both sides, I think it is important to plan ahead, so vendors should make sure that they have an incident response playbook and are, you know, participating in tabletop exercises which can help them in an incident determine what communications to share and when, and then customers too should also make sure that they include a vendor scenario in their incident response playbooks and procedures and in tabletop exercises to make sure they know what they're going to do if a vendor reports an incident to them.

And the other thing is to make sure that you know your data, so on the vendor side, you need to be sure that you know which customer's data is stored where and understanding the level of sensitive information that you're storing on behalf of customers, and then customers too need to understand what data they're sharing with their vendors.

Kattman: Lynn, What are the key findings that stick out to you?

Sessions: So, I think we've definitely seen on the contractual side of things, whether it is in a master service agreement that our clients may have with the vendors or in the healthcare setting with a business associate agreement, and as part of those contracts we have timing provisions as to when the vendor is supposed to notify the client about an incident. And again, whether we're on the vendor side or we're on the customer side of things, this can have a significant impact.

So, a lot of times we find our clients when we're representing the vendor that may very well say, gosh, I've got five days in which I have to notify my customer

of this incident, right? As Stefanie mentioned, we may not have complete information at that point in time to be able to adequately notify the customer of the particular incident. That could potentially put the customer in a worse off position, especially if they have regulatory obligations that they have to meet from a timing perspective. So, a lot of business associate agreements will also include language about a very quick turnaround, 24 hours sometimes, in which they have to notify about an incident.

And then the covered entity gets the information from the vendor and they find themselves then in a position of not having adequate information for which they can do a risk assessment. The flip side to that is if the vendor waits for a long period of time until their investigation is complete, sometimes the customers could be very upset that it took them so long to get to them about an incident. So, you can see that there is a lot of contractual considerations that need to be put in place, and I think that our clients need to be very thoughtful, regardless of which side of the vendor-customer equation they're on with those contractual obligations.

So, another thing we see is with respect to indemnification provisions, so the indemnification provisions that we oftentimes will see in contracts do not prevent the customer from getting sued and do not prevent the customer from being inquired into from a regulatory agency. So, even though there may be indemnification provisions in there, they may still find themselves under scrutiny, whether it is from a plaintiff's attorney in a class action lawsuit, or if it is from a regulatory agency in a regulatory investigation.

We see this most frequently in the healthcare space where the Office for Civil Rights investigates every incident, five hundred or more people who are impacted by it, whether you're on the vendor side or you're on the cover in any side of things, and so I think a lot of times our clients are surprised. Wait a minute, this wasn't my breach. Why am I being investigated by a regulatory body, or wait a minute, this wasn't my breach. Why is a plaintiff's lawyer suing me in a class action lawsuit. So we do see sometimes those surprises do come up from our clients because they do include these indemnification provisions in their contracts with the vendors. Stef, anything else you think we should add to that?

Ferrari: Yeah, that is a good point, and I think too in terms of regulatory investigations like you said Lynn, a lot of times our clients who were on the customer side of a vendor incident aren't expecting that investigation, so they're not getting all the materials that they usually would prepare if they had experienced their own incident, like getting a confirmation of mailing from the vendor or evidence of media notice, or evidence of substitute notice. So, I think it is really important to be sure that they're still documenting all those things as they usually would if it was their own incident.

And also on your point on notice provisions, I think not only can they sometimes put the customers in a worse off position like you were saying, but they're often unrealistic because in the first 24 or 48 or 72 hours, whatever it is of an incident, downstream contracts are not really at the top of the vendor's mind. And for

example, in like a ransomware or incident, they might not even be able to access those contracts.

Kattman: Lynn, as a customer, how can you strengthen your defense around vendor caused incidents?

Sessions: Sure, so I say vet, vet and re-vet and vet until you can't vet anymore. You need to vet your vendors, and there is a variety of different ways in which our clients do that, particularly on the security front. They are asking security questions as part of their contractual obligations. They're also following up with their vendors as they learn of new risks as they arise. So, just as you as a customer are doing your own risk assessments when you hear about ransomware matters, for example, or you hear about some type of vulnerability or some type of patching that didn't get appropriately put on systems. Then you need to be thinking your vendors may be having the same problems too.

So, especially since they're such a high target because of the number of companies that they can affect as a vendor, then they're definitely attractive to threat actors as Stefanie had mentioned earlier on. In the healthcare situation we have a lot of healthcare entities that have thousands of business associates they contract with, so those are thousands of entities, you know, hundreds certainly, and in some instances with our large health systems, thousands of companies that they contract with that have protected health information, which is that which is covered by HIPAA.

And so it creates a significant risk to the healthcare entity when they're no longer quote, in control of that protected health information once it leaves the four walls of the covered entity. So, ensure that you are vetting and re-vetting and re-vetting, and re-vetting your vendors on their security relative to the protected health information that they have in their possession. In every business associate agreement, I look at, and many MSAs that I look at these days, there is language in there about basically, when you no longer need my information, make sure you destroy it.

But what we're finding is a lot of our clients are not necessarily going back to the vendor and ensuring that that data is destroyed, so that is something else that I would put on the radar of our clients to consider. And similarly to the vendors, to be looking at the data you have in your possession, and perhaps going back to your customers and saying, hey, do I really need this data anymore?

Kattman: Stefanie, what about your thoughts about strengthening your defenses?

Ferrari: Yeah, I would just add, and we've touched on this already, but entities should make sure they're looking at their contracts with vendors and those indemnification provisions, the notice provisions, and the timing that is required there. And also the delegation provisions, so you know, who is required to notify individuals in the event of an incident? So, a lot of business associate agreements we'll see will require that the vendor perform notification, but they don't detail which notifications they're providing.

Are they providing notification to patients, regulators? Are they going to do media notice? Are they going to do substitute notice? And does the customer get a say in what goes into those notifications? Do they get to, you know, review all those materials and approve them? So, make sure you're specific in those delegation provisions in your business associate agreements because we see a lot of vendors that they want to do right by their customers, right? So, they will offer to do all of those notifications on their behalf, but we've also seen vendors who will not do any of those unless it is specifically outlined in the agreement.

Sessions: Those aren't our clients, though.

Ferrari: Of course.

Kattman: We've taken a deeper dive in the DSIR Report, which focuses on the incidents from 2021, but Lynn, could you tell us how are things looking so far in 2022?

Sessions: So, we're continuing to see a lot of vendor incidents this year, and just last week alone we had four come in on the healthcare front and two more this week, so they are here to stay. It is more of the same as what we saw about a year ago with the vendor incidents, and I think that because there have been so many of these, there is a little bit of fatigue with our client, like here we go again, we have another vendor incident that we're having to deal with. And I jokingly made the comment about how our clients, you know, are ones that tend to want to do quote, all the right things for their customers, and I think what we have seen is there have been so many vendor breaches over the last couple of years that a number of customers have seen how vendors handle these, right?

So, there is an expectation and how it is that a vendor is going to handle a breach, and so I would just say that we're continuing to see this. We're continuing to see a little bit more of a sophistication around this. Sadly, we're continuing to see class action lawsuits get filed both against the vendor and the customers. It continues to be an active space into 2022.

Kattman: Thanks so much for joining us, Lynn and Stefanie.

Ferrari: Thanks for having us.

Sessions: Yeah, thank you. It has been a pleasure.

Kattman: If you have any questions for Lynn or Stefanie, their contact information is in the show notes. Be sure to join us for our next DSIR Deeper Dive, where we will be discussing forensics in depth and the importance of proper configuration and monitoring when building your defense against security incidents. 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 of the firm. For more information about our practices and experience, please visit bakerlaw.com.