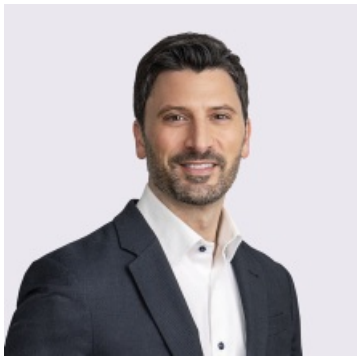
Podcast

Understanding the Post-Pandemic Data Risks

By John J. Porta & Damon W. Silver

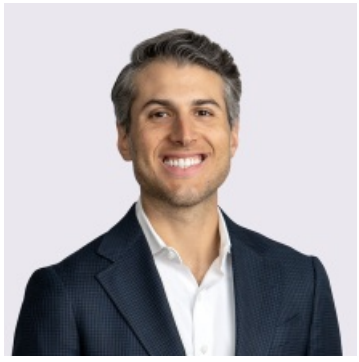
June 24, 2021

Meet the Authors



John J. Porta

(He/Him)
Principal
212-545-4043
John.Porta@jacksonlewis.com



Damon W. Silver

Principal
(212) 545-4063
Damon.Silver@jacksonlewis.com

Related Services

COVID-19
Data Incidents and Response
Employment Litigation
Privacy, Data and Cybersecurity
Workplace Training

Details

June 24, 2021

Remote work during COVID-19 presented a number of challenges including how to manage data privacy and security risks and complying with related laws that are being passed and amended at a dizzying pace.

Jackson Lewis P.C. · Understanding the Post-Pandemic Data Risks

Listen on Apple Podcasts
Listen on Google Podcasts
LISTEN ON libsyn
Listen on pandora
Listen on Soundcloud
Listen on Spotify
Listen on STITCHER
YouTube

Takeaways

Understanding the Post-Pandemic Data Risks

Remote work during COVID-19 presented a number of challenges, including how to manage data privacy and security risks when new categories of data were being collected from new sources for new purposes and during a time when data privacy and security laws were being passed and amended at a dizzying pace.

What Employers Need to Know

- Changes catalyzed by COVID-19 are likely to outlast the pandemic.
- Essential businesses and others electing to bring employees back to the office have been and will continue to collect health information about employees and need to maintain appropriate safeguards to protect that information – including when it's in the hands of service providers and other third parties.
- Data privacy and security laws in the US are governed by a patchwork of federal, state, and local laws that are often tied to the state of residence of the data subject; *not* the location of the business. Conducting business with employees and customers that are geographically dispersed can result in wide-ranging data privacy and security obligations.
- Most states require employers to implement "reasonable safeguards" to protect employee data, including by:
  - Assessing what categories of data you have, to whom that data relates, how your organization is using the information, who it is being shared with and

how long it's being retained;
    - Developing and implementing policies and procedures to protect and manage that data; and
    - Training your employees on their role in the ensuring the success of your data protection program.
- California, Virginia, and, most recently, Colorado, have passed comprehensive privacy laws – similar, in some respects, to the EU's GDPR – that grant data subjects the right to request, among other things, to access, delete, and opt-out of the sale of their personal information. We expect other states to soon follow suit.
- Laws governing the collection and use of biometric data, most notably Illinois' BIPA, require employers to provide a notice and receive consent from employees and customers before collecting their biometric information (e.g., fingerprints, scans of hand or face geometry, retina scans, voiceprints, etc.). The alleged failure to comply with these obligations has resulted in a cascade of class action lawsuits seeking statutory damages and attorney's fees.
- The transition to wide-scale remote work has led to a significant uptick in employer's use of monitoring tools to evaluate productivity and performance, manage time, and ensure compliance with company policies. While undoubtedly beneficial, these tools collect significant volumes of employee data that must be securely stored and used only in ways which avoid running afoul of data privacy laws.
- Sharing data with service providers and other third parties is an unavoidable practice, but it can expose organizations to substantial data privacy and security risk. Fortunately, this risk can be mitigated by maintaining a thoughtful vendor management program.
- If you do nothing else, make sure you:
    - Data map to get a handle on what data you have, where it comes from, how it's used, who it's shared it with, and how it's maintained;
    - Develop "low hanging fruit" policies, like Acceptable Use, BYOD, Incident Response, and Vendor Management; and
    - Train your workforce: developing policies and procedures is an essential first step, but your program will only be effective if your employees understand what's required of them and are put in a position to execute.

Transcript

Alitia (00:06):

Welcome to Jackson Lewis' Podcast, We get work™ focused solely on workplace issues everywhere. And under any circumstances, it is our job to help employers develop proactive strategies, strong policies, and business oriented solutions to cultivate a workforce that is engaged, stable, and diverse. Our podcast identifies the issues dominating the workplace and its continuing evolution and helps answer the question on every employer's mind. How will my business be impacted? For employers, COVID-19 has led to an epiphany that will likely at last, the pandemic. Work can be conducted remotely with minimal disruption in productivity and with unexpected advantages. Those advantages however come with challenges, including how to manage data privacy and security risks when new categories of data are being collected from new sources and for new purposes. And data privacy and security laws continue to be passed and amended at a dizzying pace.

This episode of We get work™ explores, why as employers plan for post pandemic life, it's critical that they include an assessment of their data privacy and security risks, and make a commitment to understanding where their exposure lies and how best to mitigate it. Our hosts today are John Porta and Damon Silver principals in the New York City office of Jackson Lewis. In his role as strategic advisor, John's approach is to emphasize the primacy of achieving the client's business goals by focusing on strategic counseling, negotiation, and risk management. Damon helps organizations of all sizes and across various industries navigate the treacherous data privacy and security landscape by assessing and mitigating the compliance risk under multiple acronym frameworks, including CCPA, HIPAA, FERPA, and the GDPR to name a few. John and Damon, the question on everyone's mind today is what do employers need to know about where employees work, the impact on collecting, using, and protecting company data and how will that impact my business?

John Porta (02:13):

Thanks Alitia. We are here today in the New York City office. This is the first time actually that we're in the same room together. So we're breaking grounds here with Jackson Lewis podcasts. This is the first podcast that we're actually in the same room Damon and I are literally less than a foot apart because we're sharing a microphone. So if you would have told me a year ago that we would have been this close to one another, or to any other coworker at Jackson Lewis, I would have been shocked. And it's interesting because we're sort of back in some way or other. One of the things that constantly as employment lawyers, we're constantly waking up in the middle of the night, especially if you're do any litigation, you're waking up in the middle of the night, gasping for air thinking, "What did I forget? What did I not provide? Or what could I have done better?"

And one of the things that's been constantly keeping me up as someone who represents clients throughout the U.S. mostly what I do is provide general employment, law advice, and counseling, but one of the things that's increasingly been coming up over the past really since well before the pandemic, but really in my practice when I'm really conscious of it is when we are advising clients on this whole other shift in the workplace what happened last year with the pandemic. Jackson Lewis went overnight from a commuter law firm to mostly remote law firm and most corporations in the United States and companies in the United States had a similar response.

So with that came a whole host of issues related to privacy and my thought process. And what comes to mind when we transitioned was, and this is not just a temporary thing, right? We're talking about we're back here today, but I think most workforces, for the most part, we're going to talk a piece about the remote work environment. But I think remote in this hybrid work environment is something that we're going to be seeing for years to come. I think gone are the days where everyone's going to report to an office five days a week. So I think whatever precautions or whatever measures companies have taken over the past year, I think are going to stick with us. And then what comes to mind when I'm thinking about privacy issues and Damon, I'm going to ask you more specifics about it, but my thought is, "Okay, remote work environment, that must raise privacy issues, right?"

And just as a disclaimer, I'm not a privacy attorney. So I know enough to get Damon involved when something seems like it's off or that I need to advise a client on something, but the issues that have come to my mind over the past year really are the transition to a remote work environment. And what sort of privacy concerns go along with that? The second time around when I thought of confidential or privacy information is health screenings, right? We're asking our employees all of this information, we're an essential business, or if we're starting to come back, we're starting to collect information, which I think is health information about our employees.

And then also, I think, we're also sharing information with third parties in this new environment. And then there's also something related to biometrics that I [inaudible 00:05:19] really understand. So Damon, with that, can you just sort of lead us into you regularly advise clients of the firm on these types of issues and you are in our privacy practice group, and really what are some of the big things over the past year that you have seen in terms of employer risks associated with the privacy of their employees?

Damon Silver (05:45):

Yeah, absolutely John. So I think a lot of what we're going to discuss today is not so much novel risk, but risk that had been accelerated and turbocharged by the pandemic, because now all of a sudden, as you pointed out, a lot of businesses like ours, that had employees that for the most part, worked from an office are now working from their homes. So some people have relocated to other states or other countries because they're now able to do their work remotely and it's more convenient for them or for their families to be somewhere else. And there are a lot of great benefits that redound both to employers and to employees from this newfound flexibility, but it does create some significantly enhanced privacy risk. One of which, and it's one that is often surprising to clients I speak with is that many data privacy and security laws are not tied to the state or the country where the business is located but instead it's tied to the location where the employee is.

John Porta (06:54):

So this is interesting Damon, and this is something that's been coming up for our clients regularly. And I think you're getting to it is this jurisdiction issue, right? So when we had the commuter workforce, everyone was reporting into the office, wherever that office was, most employers were comfortable and confident on the laws that covered them. So now, we've seen it with various different payroll taxes if somebody is in a different state, we've seen it in this situation where there's these myriad of sick leave laws that may fall into place and we've had other podcasts addressing those issues. So explain to me a little bit about how now this raises the jurisdiction and national multi-district employers who never were, are now multi-district employees. And what are some of the things that they should be thinking about in terms of what privacy rights and what privacy laws they need to comply with.

Damon Silver (07:41):

Right. So one of the key issues that employers now need to think about, because say previously, they had a hundred employees, they're all working in New York, but now

20% of them even have spread out to other states. Some of them are now in California, or they're down in Florida. The privacy laws in those states, and at this point for the most part, with the exception of a couple heavily regulated industries like healthcare and financial services, we really have in the U.S. a patchwork of state laws. So changing from one state to another, it can have a significant impact on what your obligations are. One of the key ones that comes up is do you need to provide some type of privacy notice to your employees, if your employees now in California, there's a law called the CCPA that requires a notice. It's called a notice [inaudible 00:08:32] collection, which is the disclosure by the employer to an employee or to a job applicant about what categories of personal information are being collected about employees and applicants and how the employers using that information.

John Porta (08:45):

So Damon, just so I have this straight. So basically if an employee is now working remotely, so whatever state that they're in is the law that applies not the state that the employer who's collecting the data or anything like that? So the law that's applicable is where the actual employee sits, whether it's on their couch or now on their parents' couch or in-laws couch or relatives couch?

Damon Silver (09:11):

Yeah. I mean, there are some nuances that some state laws do include language that says that the organization, in this case, the employer needs to be doing business in that state. And you could make an argument for whether an organization is really doing a business in California, simply by having one employee there. But a lot of the state laws don't include any qualifiers like that. So simply by having the employee working in say, California, if you otherwise meet the requirements to be subject to the CCPA, you could be obligated to provide that CCPA notice. California also gives employees and all data subjects, a private right of action to sue if their data is breached because the employer failed to implement reasonable safeguards. So all of a sudden, while no private right of action existed in New York, this employee by relocating to California, can now go and file a lawsuit.

A few other states also provide that private right of action. Another thing that changes is a lot of privacy and security laws create a definition of the term personal information or a comparable term private information here in New York. And what types of data elements qualify as personal information can vary quite a bit from state to state, in some states, medical information is part of that definition, meaning that if your employee's health information is compromised, not only might you have the traditional ADA confidentiality issues, but you could also be dealing with a data breach.

John Porta (10:41):

So Damon, I want to pick up on something that you mentioned that sort of gets me as somebody who's really risk averse. You said reasonable safeguards. So reasonable safeguards, this sounds like this is something like that's separate and apart from what's gone on over the past year, but when you mentioned reasonable safeguards, what is that? I'm not a classic privacy attorney, so what does that mean? And what does this mean to our clients and what they should they be doing? What should they

have already done? I guess is the question with respect.

Damon Silver (11:10):

Right. So this is a great question. And in a lot of states, unfortunately, there's really not much guidance around what qualifies as reasonable safeguards. California is one of the states that has at least given some guidance through an attorney general report back in 2016, and it's not binding, but it does make reference to a certain set of controls. And it says that a business needs to implement all of those 20 controls in order to be compliant with the reasonable safeguard requirement. But at a very high level, New York's law has kind of done this. It doesn't go on for 20 pages, but it does have a bunch of bullet points that can sort of guide you. You need to think about doing a couple of things. One is conducting a risk assessment, which essentially is at a very high level, a privacy and security audit of your information, that gives you a sense of what categories of data you have, who that data relates to, how your organization's using the information, who it's being shared with, outside parties, how long it's being retained.

And then you also need to look at what's being done currently to safeguard that information. Do you have proper controls in place to make sure that not anyone in the organization can go in and access say someone's social security number? What are the restrictions on access? Do you have a plan in place in case there's some type of breach of that information? Do you have an incident response plan? Do you have a program to manage your data sharing with outside parties? If you use a vendor to say help you manage payroll or employee benefits, you're going to be sharing some sensitive information with those vendors, or even having those vendors collect the information directly from your employees. You as the employer generally are still going to be responsible for that data.

So you need to make sure that you're properly vetting the vendors and that you are including provisions in your contracts with the vendors that are going to protect you from some type of incident, but are not going to allow the vendor to go ahead and sell that information, or to have shoddy security in place for the information, or to share it with other parties.

John Porta (13:28):

So just thinking about it. So when were talking about these reasonable safe cards, which states, I know that there's various legislation pending in states, but if you could just sort of run through some of the states that our listeners should be aware of that there's these privacy laws, because we mentioned these reasonable safeguards and that's like a best practice, right? If it's not required in the state, are we taking the position or do we advise our clients that these are best practices, even if there's not an applicable privacy law in the state that you're operating.

Damon Silver (14:03):

So in virtually every state at this point, there is a reasonable, safe guard mandate on the data security side. So just for our listeners, one point of clarification is data security and data privacy are interlinked, but with somewhat distinct concepts. Data security is preventing some bad actor from coming in and getting your data and data

privacy is the rights that are granted to a data subject, the person who the information is about which might mean restrictions on who within the organization, not some nefarious outside party, but who within the organization is allowed to access it, what your employer is allowed to do with the information. So from a data security standpoint, every state now has a reasonable safeguard mandate.

Many of them just say, in the law, you need to reasonably safeguard data. They don't tell you what that means, but almost every state has some type of requirement like that. On the privacy front, the big states are California is sort of the leader in this space with the CCPA, Virginia just passed a law that's similar to the CCPA in some respects, similar to the GDPR, which is European union law in some respects. There were a couple other states. It seems like Colorado will probably be the next that passes a law and along those lines. And then we're seeing a lot of activity in New York. New York has a law that's making its way through the legislature that's very similar to the CCPA actually goes beyond what the CCPA requires. And New York just passed a biometric law that applies to retail and hospitality businesses, and has a more generalized biometric law that's pending that would be very similar to a law in Illinois [inaudible 00:15:57] that has resulted in at least a thousand class accident litigations, maybe more.

John Porta (16:02):

I have some questions about it. So I think this is the first Jackson Lewis podcast where we actually use the word nefarious and biometric. So we definitely have the coolest podcast that we've put out there. But these biometric lawsuits, obviously we've seen them come up around the country, if you could just sort of help us to understand, and we've seen them come up in Illinois specifically, right? Can you just explain to us? Because I think it's going to have what I call the California effect, where it starts somewhere and then it sort of spreads eastward. So what are these lawsuits about for employees who are outside of Illinois? They may not have thought about this or heard about this, but can you just give me an explanation of sort of just a summary of what these laws are at, because obviously it's impacting employers and these lawsuits are being brought against employers, correct?

Damon Silver (16:52):

Right. Yeah. They're being brought against employers and also businesses in their commercial capacity. So BIPA is a law in Illinois that was passed, I think in 2008. But for a period of time after that, for years after that, there really was nothing happening. It was kind of an obscure law. And then all of a sudden in recent years, we've seen an explosion in class action litigation and the allegations essentially that under BIPA, you're required to provide a notice to someone, if you're an employer and notice your employee before you collect their biometric information, before you collect their fingerprints or a scan of their facial geometry, their retina, voiceprint, and then you need to obtain informed consent from that individual.

So after you provide the notice that discloses certain information about the biometric information program of the employer, you need to get the consent from the employee in order to collect and use information. And so these lawsuits are alleging that the employer or the business and the commercial context failed to do that.

John Porta (17:57):

Just a general question. So if that does happen, what's the exposure to an employer. I'm not saying that any employer would not want to comply with the law, but from a dollars and cents perspective, it doesn't seem as though there's any sort of financial harm to the employee. Where is the risk to employers aside from just not complying with what a law is, but what's the financial risk associated with that?

Damon Silver (18:20):

Yeah. So there's statutory damages under the law.

John Porta (18:23):

Okay.

Damon Silver (18:24):

So the employee, while it may be true, it would be difficult to demonstrate that they were harmed in some way because this wouldn't be a situation where they could say, well, my identity has now been stolen because if their is employer using it, there's not necessarily any misuse of the information, but the law provides for statutory damages. And so when you have a large number of employees impacted, you can see very significant damage [inaudible 00:18:49].

John Porta (18:50):

And is there an attorney's fees provision to these statutes, or no?

Damon Silver (18:50):

There is.

John Porta (18:55):

There is. Okay. So there you go.

Damon Silver (18:57):

It can cover Attorney's fees as well.

John Porta (18:58):

That's why we're seeing a huge-

Damon Silver (19:00):

[inaudible 00:19:00].

John Porta (19:00):

There you go. So we see that [inaudible 00:19:03] also when there's an attorney's fees provision, there is the driver on why we're probably seeing a lot of these lawsuits. Yeah. It seems to me that even that those biometrics and these types of claims I would say you're probably more at risk if you have a large hourly workforce. Right? Can you just give some examples of when would an employer be collecting biometric

information? Would it be regularly as associated with clocking in, clocking out? Where do you see this information being collected by employers? And the reason why I asked that is just because I think it's important for people who are thinking about this or listening to this podcast are like, "Oh, do we do that?' They may not think off the bat that they are collecting biometric information. So where are you seeing that with employers and how they're collecting it?

Damon Silver (19:52):

Right. So time clocks are major maybe the most common example of using biometrics, because for a lot of employers, it helps guard against the buddy punching issue where one employee is calling ahead and having their buddy clock in or clock out for them. So here with biometrics, that becomes more difficult to do. It also can be used for security purposes. In the same way that a lot of smartphones, now you can use your thumb prints, or you can use now the facial scan to gain access to your phone, you can set something similar up to gain access to your facilities or to gain access to your information systems.

John Porta (20:37):

Okay.

Damon Silver (20:37):

That's another common usage. It also can have a productivity utilization where we're again because it's biometric, and it's harder to fake, an employer could, and we have seen some examples of this use programs that allow them to see whether someone is physically in front of their computer working during the day, while they're in some remote location. And it allows the employer to keep better tabs on what people are doing.

John Porta (21:05):

Which is something that we might be seeing more frequently now that we have a workforce now that maybe wasn't always had the ability to work remotely. So we're probably seeing, and I know a bunch of clients that I service on behalf of the firm are monitoring employees more who are working remotely to see what they're doing. So obviously these are all things that sort of come out of the remote workforce, but I just want to turn a little bit now to the second piece of it, going back to sort of what are some major issues that have sort of come to my attention or make me nervous with the change in how we work over the past year and a half is we're collecting all of this information.

We're collecting temperatures. You got to take your temperature before. We have a temperature scanner. Employers are now having these daily certifications. I mean, certain states have requirements, but again, we are collecting information. So when I'm advising a client on best practices or safety procedures on what to do for clients, I'm nervous because I'm thinking, "Well, I know that this relates to privacy somehow, but how does it do that?" And what should we be doing? What are the laws? What should we be thinking about when we're collecting this type of information? And then when we're sharing it with other people.

Damon Silver (22:14):

So employers have in some contexts always collected some degree of health and medical information from employees say for purposes of a combination requests or leave requests. But now all of a sudden employers' are in the position of regularly on a daily basis, collecting health and medical information from their whole workforce, or at least our whole workforce that's reporting to the office. And while the EOC has provided some flexibility in light of the public health risk to allow employers to do that without running afoul of the ADA, the information collected still is employee medical information. It needs to be maintained separately from an employee's personnel file, it needs to be kept confidentially. And in some access restricted location, it needs to be kept secure. It's not information that should be sitting in someone's email inbox if that's the way it comes in.

John Porta (23:12):

What is this confidential information? Is it somebody's temperature? Is it I was feeling ill today, had a bad headache? What's some of the information that we should be wary of and say, listen, this is information that we need to sort of protect and what do we have to do to protect it?

Damon Silver (23:30):

Right. So an employee's temperature when we were getting regular guidance from lots of different states and localities, there were different views on whether that was particularly sensitive information. But certainly if you're getting information about an employee as symptoms and they're positive tests for COVID, a family members positive test for COVID, their vaccination status. And this is information that employers have generally been authorized to collect during COVID in some cases mandated to collect, but just because the employer is permitted to collect it doesn't mean that they're relieved of their obligation to maintain it securely and confidentially. And another key thing that employers need to think about is how can they collect the minimum amount necessary to keep their workplace secure? So this is coming up a lot in the vaccination context, where an employer is permitted to ask an employee, whether they've been vaccinated and to request proof of vaccination status, but they really want to avoid a situation where in addition to just collecting the card that says out in vaccinated, they collect other health information, or they ask an employee, why haven't you been vaccinated?

And then the employee discloses that they have some underlying health condition, or they have some religious objection to getting vaccinated, because now there's this extraneous information that no longer is directly tied to the public health consideration. And so that information is probably not going to be protected in this era. The employer is not going to be protected in the same way when it comes to that type of information and they'll have the same exposure they would if it came in by some other means.

John Porta (25:17):

So employers really need to be thoughtful, right? I know there's a rush or there's sort of an immediacy in terms of rolling out programs to protect our employees, but it

sounds like there really needs to be thought into what we're asking for, how much we're asking for and really thoughtful about what that information is. And I'm just thinking about extraneous information that you're mentioning. One final thing before I have you give me your salient key takeaways from this, just going back to when we talked about monitoring, I'm just thinking, for monitoring employees, they're working remotely. Should we be mindful of learning about information that we really don't need to learn about from an employee who's working remotely and we're monitoring them, I don't know if we're doing [inaudible 00:26:01] or whatever we're doing in terms of monitoring them. What are the things that we should be mindful of if we're doing that?

Damon Silver (26:07):

Yeah, it's a great question. And employee monitoring, particularly with our remote workforce creates a lot of benefits to employers. It may be what's necessary for them to feel comfortable having a remote workforce, but they do need to keep in mind that even if it's not their intention to collect information about say what websites their employee goes to, to look up their health condition, or what website they go to, to look up something related to their religious beliefs or their sexual orientation, or legal activities, they engage in off hours.

If you have a monitoring program that is just constantly taking screenshots of your employees' workstation, or that is keeping a log of what websites they go to, or what searches they put into Google. You now have that information, which means that if the employee sues for religious discrimination and you're in discovery, those logs may be discoverable, or your employee may have some type of privacy claim because they're going to say, "Well, you obtained this information about me in violation of my privacy rights." So employers, it's not that you can't collect it, but you do want to think-

John Porta (27:21):

You got to be mindful of it, right? You got to be thinking about exactly what information you're taking and what you're doing with that information. So Damon, one of my colleagues in California uses what are the key seduction points, right? The things that we need to be mindful of. What should we be doing? I'm in human resources, I'm in house counsel. I'm listening to this podcast and I'm a little uneasy. What are the key takeaways from this? What should Jackson Lewis clients and friends be doing best practices in order to protect privacy in their companies?

Damon Silver (27:54):

Yeah. So I think there are three key considerations there. One is data mapping. And what data mapping means is essentially creating a map or an inventory of what categories of data you have, where that data is going within your organization, who has access to it. Are you disclosing it to outside parties? How is it being used? Because honestly, without doing that, you really can't develop a sensible informed data, privacy and security program, because you don't even know what you're dealing with. You don't know what laws apply. You don't know what activities might trigger certain obligations. So that's a foundational first step. The second step is there's certain low hanging policies and procedures that you can develop that give you a high return on

investment without going too far down the rabbit hole of the data privacy-

John Porta (28:47):

[inaudible 00:28:47]. We love high return on investment. That's our favorite thing.

Damon Silver (28:51):

So a few that I recommended the clients are one acceptable use, which is a policy that essentially governs use of your information systems. And that has both a security function and also a privacy function. Second is BYOB, bring your own device even before the pandemic but especially now, a lot of employees are using their own computers, their own phones, tablets, et cetera. And you want to make sure you have a policy in place to regulate usage of those devices to make sure that you, as the employer have access to the data you need and it's being used in appropriate ways.

Third, you want to have an incident response plan. If you have some type of data breach, you don't want to first start thinking about, who do we call? Who's our outside counsel? Who's our cyber insurance carrier? Do we need a forensic contact? Who within the organization is going to lead the team? You want to have a plan in place before you want to have gone through some tabletop exercises. So this is all something that feels normal in the flow of business, and you're not in a chaotic situation.

John Porta (29:58):

So you're implementing that sort of after you pay the ransomware associated with [inaudible 00:30:02].

Damon Silver (30:03):

[inaudible 00:30:03]. Yeah, exactly. Exactly.

John Porta (30:06):

Got it.

Damon Silver (30:07):

And then the last of those sort of core low-hanging fruit policies is a vendor management policy. So this is essentially how do you figure out which of your vendors are responsible stewards of your data that you're comfortable sharing your data with. And then have you looked at your service agreements to make sure that you have the key data privacy and security protections built in that are going to require your vendors to secure your data, to only use it for purposes of providing services to you to return it to you at the end of the engagement, to let you know, if they have a data breach that impacts your data.

John Porta (30:45):

And most important for that is that they indemnify you in the event.

Damon Silver (30:48):

Yes. If you can get it to agree [crosstalk 00:30:50]. And then the final point, John is training. It's of course really important to develop these policies and procedures, but if

your employees don't know what their obligations are under those policies, they don't know what they're supposed to be doing. They're not put in a position to really execute on them. Your policies are only going to be worth the paper that they're written on. So that's sort of the final core pillar. You need the data map, you need to develop your policies and then you need to make sure your employees know what they need to do.

John Porta (31:26):

Damon, thank you. I think the purpose of today was to really, and I think you did a fantastic job. I say that probably because I'm assisting you with this but you highlighted the issues that have probably always been there, but have really now in terms of protecting our employees data and their privacy, we've identified the issues more so that have come up or sort of been brought to light on everyone's mind over the pandemic. And then we really walked through, I think some key points on what we, as employers, as in-house counsel, as human resources can do. And I think these seem to be manageable. When I thought prior to this, how time-consuming or complicated this could be, but it seems like there's a pretty good first step that we could take in order to protect our organizations. Damon from New York City, thank you so much. This is has been great and informative and helpful and appreciate it. Have a great day.

Alitia (32:20):

Thank you for joining us on We get work™. Please tune into our next program where we will continue to tell you not only what's legal, but what is effective. We get work™ is available to stream and subscribe on Apple Podcasts, Google Podcasts, Lisbon, Pandora, SoundCloud, Spotify, Stitcher, and YouTube. For more information on today's topic, our presenters and other Jackson Lewis resources visit jacksonlewis.com. As a reminder, this material is provided for informational purposes only. It is not intended to constitute legal advice, nor does it create a client lawyer relationship between Jackson Lewis and any recipient.

Trancript provided by Rev.com