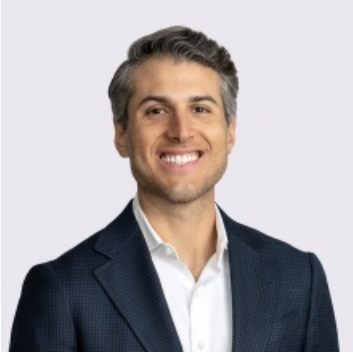
Podcast

We Get Privacy for Work: Defining Reasonable Safeguards

By Damon W. Silver & Joseph J. Lazzarotti

May 1, 2025

Meet the Authors



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

Joseph J. Lazzarotti
Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Related Services

Privacy, Data and Cybersecurity

Details

May 1, 2025

Many federal and state laws require companies to have reasonable cybersecurity safeguards in the event of a data breach, but do not specify what protections are actually required.

YouTube
Listen on Spotify
Listen on Apple Podcasts

Transcript

INTRO

Many federal and state laws require companies to have reasonable cybersecurity safeguards in the event of a data breach, but do not specify what protections are actually required.

On this episode of We get Privacy for work, we discuss where organizations should start when creating legally compliant cybersecurity policies that can withstand regulatory scrutiny.

Today's hosts are Damon Silver and Joe Lazzarotti, co-leaders of the firm's Privacy, Data and Cybersecurity Group and principals, respectively, in the firm's New York City and Tampa offices.

Damon and Joe, the question on everyone's mind today is: What are reasonable safeguards, how can my organization implement them and how does that impact my organization?

CONTENT

Damon W. Silver

Principal, New York City

Welcome to the We get Privacy podcast. I'm Damon Silver, and I'm joined by my co-host, Joe Lazzarotti. Joe and I co-lead the Privacy, Data and Cybersecurity group at Jackson Lewis. In that role, we, along with the rest of our team, receive a variety of questions every day from clients. All of which essentially boil down to the core question of how do we handle our data safely.

In other words, how do we leverage all the great things that data can do for our

organizations without running headfirst into a wall of legal and other risks? How can we manage that risk without unnecessarily hindering our business operations?

Joseph J. Lazzarotti

Principal, Tampa

On each episode of the podcast, Damon and I are going to talk through a common question that we get from clients. We're going to talk it through in the same way we would with clients. What that means is with a focus on being practical, we're going to touch on legal risks, other types of risks, options that may be available to manage those risks and what we should be mindful of from an execution perspective.

On today's episode, we're going to talk a little bit about reasonable safeguards — that lawyer term that no one really knows what it means. If you think about different frameworks, there is the New York SHIELD Act, HIPAA or the Gramm-Leach-Bliley Act. There are all of these different statutes, federal and state, and many of them refer to companies having reasonable safeguards to protect data. That isn't always clear, and the statute doesn't really lay that out, so there are a lot of questions. If you're compliance-minded and trying to figure out if this is reasonable. I don't know. Is it?

Damon, what do you think?

Silver

It is a challenging question. There's not a clear answer to it, which in some ways is beneficial because it builds in some flexibility. It seems like the intent of the reasonable part of reasonable safeguards is to account for the fact that there is a lot of variance organization-to-organization in terms of its resources, the data-related activities it engages in, the technologies it uses, how much data it processes and what types of data it processes. Part of this exercise of ensuring that you have reasonable safeguards in place is getting a handle on those types of questions. What data are you processing related to how many people? What are you doing with it? Are you disclosing it to other parties? Are you in an industry such as healthcare or financial services where there are specific requirements around your handling of data? In some form or fashion, a starting point for the exercise of figuring out if you have reasonable safeguards and making sure you have reasonable safeguards in place is doing a data security risk assessment. Really going through and starting to wrap your head around what your data risks look like.

Joe, you can talk through this a little bit. I know you've worked with a lot of clients in the healthcare space and a lot of clients that aren't necessarily subject to industry-specific regulations. What are some of the key things that you're looking for as you go through the process of doing a risk assessment with a client?

Lazzarotti

You said healthcare and risk assessment. Before getting into that, it might be

helpful to put things in some perspective. We have this term, reasonable safeguards. One of the things that I know I've talked to clients about, certainly clients that have a lot of different operations, standards and frameworks, is figuring out what to do with that. When you start to look at this issue, you realize that there are a lot of, I have used this term in the past, common threads that go through all of these frameworks.

It is helpful to think about things in terms of, and this is not something that I've created, different standards that have evolved, been enacted into law and set forth. You have administrative safeguards, physical safeguards like locks on doors and file cabinets, for example, you have technical safeguards, which are really where the IT team is strong and then you may have organizational safeguards, like agreements and stuff like that. Risk assessments might be considered part of the administrative because risk assessments could be something technical, administrative and physical. However, it's an administrative function; it's like if you're going to get insurance for a building, you have to know what data there is and where it is. Is the building made out of paper or brick? Do you have sprinkler systems? How easy is it to get out of the building? That gives you an assessment of risk. What are the threats and vulnerabilities that you have in your organization? Do you have a lot of locations? Are employees working remotely? Do you interact with consumers? Are you more B2B?

It's a process where you have a collaborative, cross-functional team that starts to look at data, what threats there are to that data and what vulnerabilities they have in their systems. You gather all of that, then look at what to do and how to address those threats and vulnerabilities. Then, ask, is what we're doing sufficient to manage that? A typical measure of risk is the likelihood that something's going to happen, and if it does happen, what's the impact on the organization? You start to look at those things, and then you start to ask, well, are our safeguards that we have sufficient, assuming they comply with the law? Do we need to do something else?

The way I like to sum it up, Damon, is to say, would I feel like I have a good story to tell if I had to stand before a judge and explain what this organization is doing? As we both know, if you have a breach, well, how could your safeguards have been reasonable if you had a breach? It is a tough spot to be in.

Silver

That's a great way of looking at it, Joe. That's certainly the argument that plaintiffs make in the data breach class actions that our team handles. However, that's not actually the case. The mere fact that there was a breach doesn't mean that your safeguards were unreasonable or inadequate. I mean, we've seen the top levels of government, the top levels of the private sector and all kinds of organizations that have extremely sophisticated safeguards that huge amounts of money have been invested in. Those safeguards are not infallible. The bad actors have a lot of motivation to find new, creative ways to get in. The fact that the breach happened is not disposed of [CG1] on the question of whether you had reasonable safeguards.

The way you teed it up, Joe, makes a lot of sense. If you do have an incident, and

you end up having to notify, let's call it 10,000 people, which would still be on the smaller end. Let's say it's a healthcare entity that has to report to OCR or a different type of entity that has to report to the State AG. That agency is investigating the breach, and then you get some class action litigation related to the breach. How are you going to feel about the safeguards that you had in place? Equally importantly, are you going to be able to demonstrate that you had those safeguards in place?

We work with a lot of clients where if you have a discussion with them, certain members of the organization will say, absolutely, we have safeguards in place to address this, that and the other things. Then you ask for any documentation demonstrating those safeguards, and there's nothing or it's very piecemeal. Someone has put together a Word document on this particular area at this point in time, and when you pull all of that together, it doesn't make a very impressive showing for OCR or a State AG. It doesn't look great in discovery and litigation. The truth is, oftentimes the absence of a written policy is an indication that the safeguard probably isn't in the place that the organization may have thought that it was. Going through the process of developing the policies and procedures helps you from both standpoints of:

1. It is legally required.
2. It is what will allow you to most effectively push back on the investigation or defend yourself in litigation.

It can also be helpful just in day-to-day business. We see increasingly that parties with which your organization may do business want to see your written information security policies as evidence that you have a good program in place. Also, having to go through this process of doing the risk assessment, developing policies and procedures and committing to writing what you're doing, oftentimes has the side benefit of helping you see that maybe things are not where you thought they were. It helps you to plug some of those gaps and to think through what makes most sense in terms of how to protect yourself going forward.

Lazzarotti

Flesh that out a little bit more. One thing you said made me think about something: What is a good place to start, right? Some people listening may say, well, alright, guys, that sounds all nice, but what do I do? What do we do? A good place to start is to say, okay, if you're in a regulated industry or maybe you're in New York, Massachusetts or a state where they have fleshed something out. Start with that. What is that set of rules, that industry guideline or whatever it is, start with that. In other words, because you comply with the state law or a federal law that governs you, number one, that state law or that federal law may only apply to a certain part of your data. It may not apply to all of the data that you have that requires safeguarding.

What's the thinking around, do we need to do more than what a particular statute that regulates us requires?

Silver

It's a great question. Starting with one of the points you mentioned, it can very often be the case that there are different legal frameworks that are going to apply to different types of data that you maintain. So, probably the easiest example to illustrate this is you're a hospital, your patient data is subject to HIPAA, but you also have employees. Your employee data is generally not subject to HIPAA, but is likely subject to state law that says you need to have reasonable safeguards in place to protect an employee's social security number or their bank account information.

It is important not to, and there is an understandable tendency to try and paint with a broad brush and say, this is our program that will apply to everything equally. Maybe at the end of the day, you do it for administrative simplicity purposes and want to have some overarching set of policies. However, the starting point has to be looking at it in a more segmented way, and making sure you understand what the standards that apply to us are.

Then, to your point about whether just doing what the standards say is enough. A lot of times, the standards like HIPAA are somewhat detailed. A lot of times, the standards, for example, the Massachusetts regulations and the New York Shield Act, are pretty high-level. They tell you, generally speaking, the types of stuff you're supposed to do, but they don't get into the level of detail that you're going to need to get into as an organization to actually have those safeguards in place. They may say you need to have an access management policy, but what does that actually mean? How are you actually going to go through the process as an organization to determine what types of employees should have access to which databases, and make sure that when an employee leaves or changes positions, that access is cut off? You really do need to think about it in a way that's tailored to the way that you are doing business. While there are certainly principles that carry over from organization to organization, for any of this to be effective, it has to be mapped onto what you're actually doing.

On that point, Joe, how is that something you try to help clients think through? What is the way to jump from what the standards may be under a legal framework or best practices to what makes sense for this particular client's business?

Lazzarotti

There are a couple of things that come to mind, Damon. One is, we talked on a number of occasions about cyber insurance and how important that is. You may think about what if we went out to get our policy updated, and what the requirements would be of a carrier? What makes us more attractive insured, even though you comply with that standard? For example, New York doesn't require multifactor authentication, but we all know that multifactor authentication is a pretty well-established control that people would expect you to have. Does not having it mean you're negligent? I don't know. That's not for us to decide, but it might be something that's important and valued by a carrier for underwriting purposes. You might look at that and say, well, if we want to be better insured, let's make sure we have that particular control in place.

You might look at what your clients require. Some clients will say, you need to

comply with all laws. Thank you; that gets us back to the same place of reasonable safeguards. Then, you may want to go beyond that and say, well, what does that mean? Well, that means you're going to do an annual risk assessment, or you're going to have an incident response plan. We talked about that. You're going to have multifactor authentication, and that's listed specifically in the agreement. Now, you know if I want to get business from this company, I'm going to have to do these additional things beyond what my state law requires.

If people say, well, look, I want to sleep at night, Data breaches can be pretty disruptive, pretty upsetting and scary in some cases. It's difficult to get through that and people don't want to go through that. No system is perfect, but if you start to look at your environment, as you were suggesting at the outset, in terms of what kind of data, how much of it and how sensitive it is. You may start to say, we really need to tighten it up. Maybe we need to have encryption at rest or in transit, and put some more locks down in terms of what employees can do and access. A VPN — having that certainly required and not just having MFA, but forcing people to use it. There are things that you can really tighten up, but that's a matter of risk, so really understanding your risk and reacting to that in a reasonable way.

The reasonableness also plays into it in HIPAA and in other laws. What's the cost of that? Can you feasibly incur that cost to implement and maintain these higher-level controls? It's a real factor that we don't want to ignore as we go through. Those are the things that I would try to think about in deciding what steps to take beyond a particular framework.

Silver

That makes a lot of sense. We did, on a prior episode, discuss this in the context of incident response plans. It's equally important in the context of having reasonable safeguards in place. You can do the risk assessment and have your written information security manual, but then there's the part of actually being able to execute.

That really does come down to employee training and having that employee training be role-based. In other words, having training that is tailored to specific types of employees based on what they are doing with respect to processing your data and helping make sure your safeguards are in place. We have worked with many clients who have a very impressive-looking 120-page WISP (written information security program), but no one has looked at it in years. A number of the frameworks we've talked about, like HIPAA and the Shield Act specifically, say you have to regularly train your employees on these policies and procedures, and help them understand what their role is.

Joe, maybe to close this out, do you want to talk a little bit about what we do when we're working with clients on providing this type of training?

Lazzarotti

It depends, obviously, on what the client wants, what they feel is helpful for their team and who they feel needs to be trained. There are really two approaches we take. One is to just educate employees about the risks and the kinds of things to be

mindful of, what the laws are and what's required under the laws for the particular company and that particular group that we're talking to.

Then, as Damon was saying, he used the term role-based because each employee may serve a particular role, and certain policies may apply to that employee. The idea is, it's not what any company should do in the event of a breach, for example, to use that. We say it's what the company has determined they want to do. That's really the training part. Helping the employees to know this is what this company has established as the safeguards we want our employees to follow. It's one thing to just talk about, well, know, HIPAA requires an access management policy, an incident response plan and this, that or the other thing. However, that's not necessarily how the company has brought that into its organization and operationalized that particular requirement for that particular group. That's a little bit more of a detailed training where we would, in a case with a client, we would want to understand first, well, what are you doing? What's the policy? What does it say? What should we focus on? Then, really talk about what the company requires. Let's go through it.

Silver

I agree with all that. One thing to layer on there is we found it's been very helpful in a lot of these trainings to have hypotheticals to work through with the audience. In addition to making sure that the discussion of policies aligns with what the organization is actually doing, we want to make this information accessible to the attendees of the program. A lot of times, when you talk about a certain concept, say data minimization, access management, getting authorizations for disclosures or spotting phishing emails, it can be a little difficult for people to understand how that is going to come up for them in their day-to-day. It is also just hard for them to absorb the information. We found that when we work through hypotheticals and specific scenarios that employees in that particular group are likely to face on a somewhat regular basis, all of a sudden, people's eyes light up. They remember that happening, or they could see that happening, and they understand why the policy exists, and what they're supposed to do in the event that they find themselves in that scenario.

Lazzarotti

That's exactly right. At the end of the day, all the things we're talking about, this idea, just to bring us back to what's reasonable, it really depends on a lot of factors and what's right for the organization. Sometimes it's good to talk about that with people who are outside the organization, who can help you determine whether you may think this makes sense, but you may have a tough time defending that and getting to what is more likely to be objectively reasonable.

Just to close this one out, hope everybody's being reasonable. If you're listening to We get Privacy, you're being reasonable. Just a joke. Thanks for listening. If you have any other topics that you'd like us to cover, you can email us at privacy@JacksonLewis.com. Damon, always a pleasure.

OUTRO

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 to on Apple Podcasts, Spotify 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.