Podcast

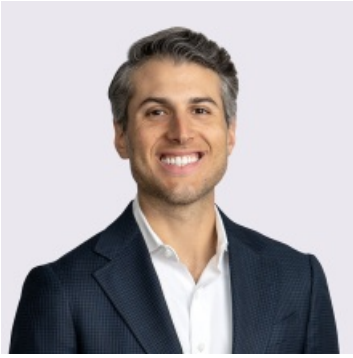
We Get Privacy for Work: Why You Need a Cybersecurity Incident Response Plan Now

By Joseph J. Lazzarotti & Damon W. Silver

April 17, 2025

Meet the Authors

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



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

Related Services

Privacy, Data and Cybersecurity

Details

April 17, 2025

As states increasingly introduce legislative requirements for how companies respond to cybersecurity threats, it is more important now than ever for organizations to have a plan in place to address data breaches if and when they occur.

YouTube
Listen on Apple Podcasts
Listen on Spotify

Transcript

INTRO

As states increasingly introduce legislative requirements for how companies respond to cybersecurity threats, it is more important now than ever for organizations to have a plan in place to address data breaches if and when they occur.

On this inaugural episode of We get Privacy for work, we guide organizations through the process of creating an incident response plan, including who should be involved and how to effectively notify stakeholders.

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: Why should organizations have a cybersecurity incident response plan, what should be included in the plan, and how does that impact my business?

CONTENT

Joseph J. Lazzarotti
Principal, Tampa

Welcome to the We get Privacy podcast. I'm Joe Lazzarotti, and I'm joined by my co-host, Damon Silver. Damon and I co-lead the Privacy Data and Cybersecurity Group here at Jackson Lewis. In that role, our colleagues in the group and we receive a variety of questions every day from our clients, all of which 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 unreasonably hindering our business operations?

Damon W. Silver
Principal, New York City

On each episode of the podcast, Joe and I are going to talk through a common question that we're getting from our clients. We're going to talk through it in the same way that we would with our clients, meaning with a focus on the practical. What are the legal risks? What options are available to manage those risks? What should we be mindful of from an execution perspective?

Joe, our question for today is, what is an incident response plan, and what should it include? To set the table for everyone, do you want to just talk a little bit about what an incident response plan is and what purpose it serves?

Lazzarotti

That is a great place to start. For a lot of organizations, when we talk about an incident response plan, there are a lot of different incidents that a company may face or crises that they may encounter. I'm here in Florida now, and hurricanes may be incidents that people might have a plan for, but we're talking specifically about security incidents. Data breaches and things that may impact the organization's systems and ultimately result in some access or acquisition of personal or confidential company information that may create legal obligations to provide notification in certain cases— whether that be to federal or state governmental entities, individuals who are affected, customers or whatnot. These plans can sometimes become pretty complex, depending on the organization, particularly if you're in a highly regulated industry, but we're going to try to talk about it at a high level.

For me, one thing that is pretty critical in the event of an incident is understanding how to communicate with the people who need to carry out that plan. That can be difficult. Bad guys have gotten into the system, and maybe they're still in or can be monitoring email, or maybe the company's email is not able to function at the moment. How do you communicate with people? So, having that alternate communication strategy can be pretty important, and having a plan for it is critical.

Silver

Related to that, we see all the time, especially with clients who haven't been through one of these incidents previously, that they're not really sure who the people who should be involved are, both internally and externally. If they haven't been through this situation before, for example, if someone just happens to be the manager who finds out from an employee about a link they clicked on, a suspicious email they got or about the fact that they lost their company laptop. An important first step is for them to know who they are supposed to go to report this. Then, the person who receives that report needs to know whom they need to assemble. Who are the right people internally to be tasked with managing this?

There's sometimes a misconception that it's just going to be an IT function, and the IT department is going to handle it. Really, in a lot of these instances, the incident has a much broader impact, and IT alone is not going to be in a very good position to respond. You're going to need people with a legal perspective. You might need people with an HR perspective if employee data is impacted. You might need people from the finance team if accounting data is impacted. You're definitely going to need somebody or multiple people from leadership who are able to make decisions at the highest level for how the organization is going to respond.

Then, there's also your external team. Your legal counsel can, under the cloak of privilege, help you do an investigation of the incident and assess your legal obligations. You might have a cyber insurance carrier or broker whom you want to put on notice quickly. You might have a digital forensics firm that you want to have on standby who understands your systems and can jump in quickly.

Knowing who those key players are helps make the process much smoother when something like this happens. Depending on the nature of the incident, it could be pretty chaotic in those early days. That's not the time you want to try and figure out who's supposed to be involved and, to Joe's point, try and figure out how those people are going to communicate.

Lazzarotti

Absolutely, the roles and responsibilities of the individuals are important. One other thing, and this is not specific to the content of the plan per se, but you said something that made me think about it, Damon. What if you needed to get a copy of the plan and your systems are encrypted? So, where do you keep this plan and the contact information of the individuals who are on it? How do they know that they're on this plan? So, these other things that come with what should be in an incident response plan. It's also about socializing with those people, maybe doing a tabletop exercise, and keeping the contact information in a place that can be accessed.

Certainly, you mentioned your cyber insurance carrier; that's really a critical piece of helping to respond to these incidents. Not only from the standpoint of providing resources in terms of having the policy pay for certain expenses that are incurred but also having gone through and helped to identify those external parts of the team that Damon referred to that will help in responding to the incident. Suppose you go out for renewal on a new cyber carrier the following year because you feel like you need to make a change, but they have a different set of people on their external team. Does that mean you have to update that in your incident response plan?

Some of the things that we're talking about are things that you have to keep up to date. It is not something you just prepare, leave on the shelf and don't actively use. A lot of this is about preparedness, and these plans can really help improve that position of being prepared, in addition to keeping the system secure. It's really both of those. That's what I'm seeing.

Silver

I totally agree, Joe. Honestly, there is value in the plan itself. It is, in many instances, a legal requirement to have the plan. Even more important than the document itself, in most instances, is building that muscle memory and going through the process of thinking through incidents. You do want to be specific about what type of incidents you think you're most likely to face. You mentioned the example of a hurricane that knocks out your power, or there could be a ransomware attack or a business email compromise. If you have employees that work remotely or travel, you do want to think about those lost laptops, lost phones and other devices. If you have a website that potentially, let's say, has customer accounts that store sensitive information, there could be some type of misconfiguration of your website. There's a lot of value in thinking through the scenarios we are most likely to face or that would have the biggest impact if they happened.

Then, what are the steps we'd want to go through if those specific types of incidents happened? How do we make sure that our team is not trying to fumble around and find this plan, read through it and go step by step? In reality, that's not how it's going to play out, particularly if it's a ransomware attack or some other type of event where you're trying to respond quickly and things are feeling chaotic. You want people to have practiced this enough that they're just acting on the plan and remembering at least key components of the plan. They're likely not going to be in a position to go through it, so first, start reading up and trying to understand what the plan contains when there's an actual incident. That piece of practicing on a regular basis and having key stakeholders involved in developing the plan is more important than the plan itself at the end of the day in terms of the value it can provide to you when responding to an incident.

Lazzarotti

That's exactly right. Related to that, we are seeing clients who want to have all of the state laws available and exact drafts of notifications. To some degree, that really is a good idea because if you have a sample notice for an individual or a sample website notice, in the event you needed to put something out there, you would be in a better position. If you had some talking points for key people in the organization, some FAQs for a call center if you have a need for that. Those are all good things to have as a starting point.

However, to Damon's point, when you're in the situation, the circumstances are going to dictate things that you just might not have anticipated, or you're going to need to tailor those sample tools that you've made a part of your plan to the actual circumstances. You don’t have to worry so much about everything being perfect because the situation is going to take you in a direction you just may not have anticipated, but at least you'll have really good starting points that will speed the process along so that the plan can be useful for you when it's needed.

Silver

Well said. We've laid the groundwork pretty well conceptually for what purpose these plans serve and how, from the standpoint of using them, a lot of the work is done at the front end before you actually have an incident.

When you're working on preparing a plan or reviewing an existing draft of a plan, Joe, what are the most important types of things that you're looking for?

Lazzarotti

For me, it's clarity, usability and functionality in the sense that if there's an incident response plan that is 40 or 50 pages, I'm looking at that saying, that seems like a lot to work through. You always want to be careful, and people may have put a lot of thought into it. What I'd recommend in that case is saying, why don't we do a high-level summary, a checklist or something that is coupled with that large, well-thought-out plan that can be more action-oriented in a situation.

The other thing is to make sure that it covers all of the aspects of the business. One of the things that you said at the beginning is that, sometimes, this function gets pushed to the IT department. However, the IT department may focus on an incident response plan more from an IT perspective. How do we deal with the information system that's down? What gets left out of that is how we communicate about it. How are our clients affected? Do we have contractual obligations and all that other stuff that may be relevant to the overall response? So, I'd want to be sure that the incident response plan really covers the whole organization, which may include HR, other business units or even wholly owned subsidiaries that may be the parent or even maybe a franchisor. It's not directly their business, but they want to understand, and we have to protect the brand because there could be those kinds of issues. So, really give some thought to whether the plan is really going to help us. Is the plan as broad as we want so that we're able to act on it in a situation?

Silver

I agree with that. Thinking about the high-level summary or the checklist that you mentioned, I've had similar discussions with clients about how to leverage the work that was done to create a really detailed plan. Also, it's good to have some more accessible, actionable documents to work off of and keep you organized as you're responding to an incident.
What are some of the key items on that checklist for you?

Lazzarotti

How do you communicate with folks? Who do you need to reach out to? If you are a professional service firm, you need to notify your clients. Where do you go for that information? How do you assess what obligations you have? A lot of focus is on data breach notification laws, which we're involved in a lot at the federal and state levels. However, there are increasing contractual obligations. Sometimes, it can be difficult, like where are those contracts or what obligations do we have? Having that available, or at least a path to them that you can easily access, can be helpful. Obviously, your broker and carrier— know how to contact them and how to get to the sample forms that you need. Those are some of the things that I'd like, but there are other things.

I'd be interested, Damon, in knowing how you might augment that list.

Silver

I agree with all of those. In some ways, it all starts with a triage list of what your objectives are early. You learn that some type of incident has happened; now, what are the first several steps that you need to take? Those are going to be the most pivotal from the standpoint of the incident response plan having value because those are the things you're going to have to do potentially very quickly and without much opportunity to deliberate or to reach out to your attorney and run it by them. These are things that need to be done quickly, and it is going to vary depending on the organization. It's also going to vary depending on the type of incident, but sometimes, if we're dealing with something like ransomware, a big initial question is how do we get our business back up and running? We're going to want to look at whether we have backups that we can restore from or if those backups were impacted by the incident. If we don't have the backups, what other options do we have? Is there any type of publicly available decryption tool, and who do we go to try to explore that? That's one early question, at least for certain types of incidents: How are we going to get our business back up and running?

Another key early question is how do we make sure that we're going to be able to do the investigation that we want to do with this incident? Because I know both of us and other members of our team have seen many instances where the client's internal IT or a managed service provider took some steps really early on in the process that resulted in the wiping of logs that otherwise might have been useful in showing that the scope of an incident was narrowed to certain systems or certain files, but those are wiped. So, the client is left in the position where they may have to make assumptions about what could have been impacted, which results in a much broader notification than might otherwise have been the case.

Of course, another consideration is whether this incident is over or if it is a live incident. Is there still a continuing ongoing threat to the systems? What needs to be done from a containment perspective? Having those pieces spelled out clearly and in a practical way with actionable steps that people can take are going to be really important so that in those early moments, you don't have issues that set you back weeks in terms of getting back up and running or set you back indefinitely in terms of losing evidence. All of those can be really valuable to spell out and also, again, looping back to the point of practicing to have people think through plans in connection with specific types of incidents that might come up.

Lazzarotti

I think we could probably talk forever about writing an incident response plan. One last question, Damon. Once you do have a plan and are practicing that plan, how often do you think a company should revisit and amend it if needed? How often should you review it and consider updates?

Silver

It's a great question. It's going to vary depending on the client's circumstances. A really valuable exercise is to have a standing time on the calendar to look at it. If it's every 6 months or even every 12 months, have that meeting scheduled.

Then, if something happens, like you experience an incident or you're integrating some new technology that's going to process a lot of data, that might be a good

reason to either have that meeting sooner than was planned or to have an additional meeting because this really does need to be a living document. It's not going to serve you very well if it just remains static over time. Putting that time on the calendar ensures that, at minimum, every 6 months or every 12 months, you're giving it a look to see whether it still makes sense in light of the way that you're handling data, and you have that opportunity to make corrective actions if that's necessary.

Lazzarotti

That sounds great. I definitely hope all of our clients are thinking about this, and if they don't have an incident response plan and are developing one, this session will give them some thoughts about that. We hope everybody enjoyed listening to our We get Privacy podcast, and thank you, Damon.

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, Libsyn, SoundCloud, 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.