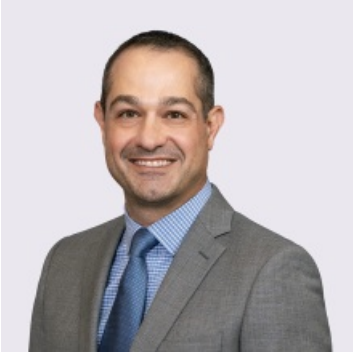
Podcast

What to Include in an Incident Response Plan

By Jason C. Gavejian & Damon W. Silver

October 23, 2023

Meet the Authors



Jason C. Gavejian

Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

Damon W. Silver

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

Related Services

Cybersecurity Awareness Audio Guide

Details

October 23, 2023

In today's digital world, it is unfortunately more likely than ever before for an organization to be faced with some type of data breach crisis. When that happens, data incident response plans are necessary—and invaluable. Having a well-thought-out plan is the best way organizations can prepare for managing those events quickly, in an organized fashion and with the goal of minimizing any potential risk.

Jackson Lewis P.C. · What to Include in an Incident Response Plan

Listen on Spotify
Listen on Apple Podcasts
YouTube
Listen on Soundcloud

Transcript

Alitia Faccone:

Welcome to Jackson Lewis' podcast, We Get Work, focused solely on workplace issues. It is our job to help employers develop proactive strategies, strong policies, and business-oriented solutions to cultivate an engaged, stable and inclusive workforce. Our podcast identifies issues that influence and impact the workplace and its continuing evolution, and helps answer the question on every employer's mind, "How will my business be impacted?"

In today's digital world, it is unfortunately more likely than ever before for an organization to be faced with some type of data breach crisis. When that happens, data incidents response plans are necessary and invaluable. Having a well-thought-out plan is the best way organizations can prepare for managing those events quickly in an organized fashion and with the goal of minimizing any potential risk. On this episode of We Get Work, we discuss the benefits of having a well-crafted plan, defining containment, investigation and communication, and what key steps organizations should take when developing their plans.

Our hosts today are Jason Gavejian and Damon Silver, Principals in the Berkeley Heights and New York City offices of Jackson Lewis and core members of the Privacy, Data and Cybersecurity practice group. Jason co-leads the group and is a certified information privacy professional with the International Association of Privacy Professionals. Jason's work includes counseling international, national and regional companies on the vast array of privacy and security mandates, preventative measures, policies, procedures and best practices.

Damon has led investigations of and responses to dozens of data breaches. He has successfully navigated the resolution of numerous investigations by government agencies like the Department of Health and Human Services and State Attorneys General. Jason and Damon, the question on everyone's mind today is why is having a data incident response plan essential and how does that impact my organization?

Jason Gavejian:

Thanks for joining us. Today we're going to talk a little bit about data incident response plans. An incident response plan is really an invaluable resource for your organization in today's digital landscape. The best way through any crisis or disaster is to have a well-thought-out and practice plan, whether that's a fire drill, I think we've all been through plenty of those in our lives, or developing a specific plan for how an organization is going to deal with an incident response or a data breach, the cleanest way forward is to really understand that we need to prepare for the worst in order to get through those inevitable events quickly and in an organized fashion.

When we're faced with an incident that impacts the business datas or personal information your organization regularly collects or shares, a well-crafted plan is going to serve as your roadmap. It's going to guide your organization through the chaos that is inevitably going to come, and it's going to help you define steps for containment, investigation and ultimately communication. By promptly identifying and mitigating the breach, your organization is going to be able to demonstrate the diligence that it's spent in preparing and potentially minimize fines, penalties and/or the threat of litigation on the backend.

Really swift transparent communication as outlined within your plan can also really help salvage a company's reputation, which is going to be crucial in an era where data privacy is a paramount concern for our consumers and frankly, something that more and more consumers are becoming mindful of. In essence, a data incident response plan is going to be the legal groundwork to help you mitigate damages, satisfy regulatory requirements, and safeguard the reputation of your business in the face of a data breach. It's going to be your proactive legal strategy that every organization should have in place.

So Damon, the first 24 to 72 hours after an incident can be critical to successfully recovery and from an incident response or the incident response plan that you're going to ultimately implement in connection with the incident. So how can an IRP or incident response plan assist organizations to put their best foot forward during that initial phase?

Damon Silver:

Yeah, so Jason, as both of us have seen firsthand many times, that first 24 to 72 hours can be really intense. There may be major disruption to business operations. There may be demands from internal and external stakeholders for information. There may be rumors circulating about what happened and what the impact will be. And with all that going on, it's very easy for the organization to experience the incident to start making some bad decisions or to miss out on opportunities to

mitigate risk.

Having an effective instant response plan in place can certainly help with all of that. As you pointed out, there's some degree of chaos that's unavoidable, but an instant response plan can help you sort through some of that chaos and process things in a more systematic and methodical way. So for instance, one of the key things an instant response plan will do is to identify the key members of your response team, both internally and externally, so that one, those team members in advance of an incident can be appropriately trained, they can go through tabletop exercises, and also along similar lines, so that you have clarity around who's responsible for what aspects of the response, and there are a lot of different balls in the air at once.

So for instance, it's helpful to know who is going to be the person who reaches out and coordinates with your cyber insurance carrier? Who's going to liaise with outside counsel? Who's going to be responsible for handling and vetting internal communications about the incident? On the internal side, and that this will be somewhat dependent on how your organization set up and the size of the organization, but oftentimes you're going to want to have a team that includes members of legal and compliance departments, leadership, and then depending on the nature of the incident and what data or systems seem to be impacted from people from relevant business units and/or from HR.

And then on the external side, some of the key players on the team are typically going to be outside data security counsel, a digital forensic incident response firm, and of course your cyber carrier. And basically the way, and there's a lot of overlap, but the way the delegation of responsibility for these outside advisors will typically break down is you're going to have outside counsel quarterbacking the operation, seeking to preserve privilege advising on the legal consequences of the incident. You're going to have the digital forensic incident response firm leading the charge on remediation and sorting through the forensic evidence to determine what data was impacted. And then you're going to have the cyber carrier, hopefully, depending on the specifics of the incident and the policy, providing some level of financial support and helping to marshal the right resources.

Another area where an incident response plan can be very helpful is instructing people within your organization on where they should be directing information about the incident, so that that information's making it into the hands of the right people. We've definitely seen unfortunate situations where critical information got lost in that chaos that Jason mentioned, and as a result, there may be blind spots in the decision-making by the incident response team.

Another thing an incident response plan can do is outline the key steps you're going to want to try and take to preserve attorney-client privilege over your investigation, and also to preserve forensic evidence. So on the attorney-client privilege front, the key action item is going to be getting outside counsel involved right at the outset so that outside counsel can make sure that it's structuring the investigation properly. For instance, that it's engaging the digital forensic incident response firm on your behalf and participating in communications regarding the investigation so that you're in the best position possible to argue that those communications are subject to privilege.

And then on the forensic evidence side, the key is to avoid this, which seems to be in many cases, an irresistible urge to wipe the systems that were impacted by the data incident. Instead, what you really want to be doing is working through counsel to engage and experience digital forensic incident response firm who can come in and then help you start balancing between the need to, of course, secure your systems and try and get yourself back up and running, but also at the same time, the need to preserve evidence so that when all the death settles, you are able to get a clear picture of what transpired. We're going to cover this a little bit more later in the discussion here, but give you a clear picture of what transpired so that you have the information available that you'll need to assess what your obligations are stemming from the incident from a legal standpoint.

So Jason, once you get through those first 24 to 72 hours, what are some of the key steps that come up next on the incident response checklist?

Jason Gavejian:

Yeah, so just one point real quick, Damon, is with respect to identifying your internal team, there's the old saying, "Too many cooks in the kitchen," you're ultimately going to want either one person or two people who have responsibility for running your incident response plan. If you have 30 individuals identified as your key decision makers, chances are when you're trying to make decisions on an hour or sometimes on a minute by minute basis, you're not going to be able to move effectively through the incident response process if you have too many individuals as part of that decision-making or core decision-making team.

So again, just thinking about having overall responsibility or a limited number of individuals with overall responsibility will be key. So once you put your incident response plan into action, your team is really going to be triaging next steps. In particular, you're going to want to make sure that the operation is back up and running as quickly as possible. This is going to help you to minimize any potential loss of revenue due to business interruption. How you go about doing that is really going to vary from incident to incident and will certainly be impacted by any of the steps that you've taken ahead of time to prepare for such an incident.

In particular, if your data has been encrypted or corrupted, the first question that you're going to want to know is whether or not you have good data backups and are you able to restore your systems from those backups? And if you are able to restore just how long it's going to take your organization to get back up and running? If you don't have good backups, you may need to pay the ransom or make some alternative arrangements to minimize the time that your business is not operational.

At the same time, your incident response plan should specify for the collection and analyzation of the forensic evidence. That's going to be critical in helping you to determine whether or not the incident triggers any notification or reporting obligations. That forensic investigation should also attempt to determine whether or not there are any indicators of compromised, unauthorized data access or acquisition within the environment. And if so, what data may potentially be impacted?

This investigation's also going to help you determine if there's any problematic gaps in the forensic evidence that's already being collected. As Damon mentioned, it's really critical that that forensic investigation be under the attorney-client privilege so that we can eventually preserve the argument if we ever need to in a litigation or similar type environment.

Further, you're also going to want to consider how and what you're going to be communicating, whether that's internally and if needed, and are perhaps even required under the law, externally about the incident. While each of these points should be covered within your incident response plan, they should be discussed in relatively general terms. That's going to allow your team some flexibility to work through the unique nuances of a particular incident.

So Damon, assuming that there are indications of unauthorized access or acquisition, what are the next steps in the process?

Damon Silver:

If you are seeing those indications, and typically it's going to be through your discussions with the digital forensic incident response firm coordinated by counsel, they're going to, for example, look at activity logs and they may see some evidence that the bad actor at the very least had access or had the opportunity to access some of your data. So assuming that's the feedback you're getting from your digital forensic firm or your internal team, your instant response plan should outline, and I totally agree with Jason at a high level because there are a lot of nuances, but it should outline how you're going to answer three key questions.

So the first is, does that data that appears to have been impacted qualify as personally identifiable information or PII? The second is, does the incident qualify as a, "Breach?" And I say quote-unquote because a lot of times there's a tendency to think that if there is some type of security incident, that automatically means there is a data breach. But a data breach is actually a term of art defined in statutes. That definition varies by jurisdiction. So it may not be the case at the end of the day that this data incident resulted in a data breach. And as lawyers, we always right from the get go, caution our clients against describing the incident, particularly in writing as a breach because of the legal connotations that carries.

And then the third question you want answer, if your answer to those first two questions is yes, if yes, it looks like PII may have been impacted, and yes, the incident qualifies as a breach is what notification and reporting obligations were triggered as a result? Answering these questions requires case specific analysis based on the evidence from your investigation. In particular, you'll need to drill down on what specific data elements were impacted, because as I mentioned, the definition of PII varies by jurisdiction, although there are some data elements that are going to be PII, no matter what laws are governing the incident.

So for example, if security numbers or driver's license numbers or financial account information in combination with the security code or access code or password to access that account were impacted, you're very likely dealing with PII. But then there are other data elements like biometric

information or medical and health information or online account credentials that are PII in a growing number of states but are not PII in all states. So you really do need to get granular, which oftentimes requires a process called data mining, where you run search terms through the dataset and then manually review the hits to see what specific information was impacted.

Another thing you need to do, oftentimes through that same data mining process is figure out who the specific data subjects were? Who the people that the impacted data relates to were? Both because if you need to notify them, you of course need to know who they are, but also because the state in which those individuals reside may dictate what laws are going to govern your response. We've seen many instances where we had a client that only operated in one state, maybe even just one single location, but given the nature of their business, they had data relating to people all over the United States and in other countries as well. And so a lot of times you can end up with a very wide-ranging set of legal obligations you need to navigate even if the business itself is pretty localized.

And then the last thing you want to start wrapping your head around based on your investigation is how specifically did the unauthorized party interact with your impacted data? For example, are there indications that they exfiltrated or stole copies of your data? Or on the other hand, do we just see evidence that maybe they got access to an email account or to some application that stored your data, stored your PII? But maybe it's the case that they only had access for a brief period of time.

Sometimes we'll see in a business email compromise that the bad actor only had access to the email account for six minutes. And in that case, although you may not know for sure what specific information they accessed in the six minutes, you have a reasonable basis to infer that they couldn't have accessed a whole lot. So that's some of the information that your instant response plan, at least at a high level, can outline for you to make sure that you are checking the box on as you discuss the matter with your counsel, with your digital forensic firm and with the other players involved.

Jason, I alluded to this a little bit, but there are a lot of different laws that come into play, and it can definitely impact what your investigation and response look like. So could you just very quickly give us an overview of what some of the key laws are that govern whether notification and reporting is required, and also what some of the key considerations to be mindful of are if you are preparing notices and reports?

Jason Gavejian:

Yeah, absolutely Damon. So some of the key laws or regulatory frameworks that we want to be mindful of and which your incident response plan should really discuss, and they're going to depend on your industry and certainly depend on the nature of the data that you're going to maintain, but they might include HIPAA, the SEC, as well as the various state data breach notification laws. As you mentioned, Damon, each state has its own data breach notification laws, and those laws are

meant to protect state residents. So even if you are in one particular jurisdiction but you maintain information about residents of a state other than your own, you're going to need to be mindful of what that state law says and what it might require in the event of a data breach.

Timeliness is also critical as many regulations or laws in the space emphasize the importance of prompt notification. It's also critical, as you mentioned, to ensure compliance with some of the content requirements under various state law. That's going to create some challenges as you need to be consistent with any of the prior communications that you may have issued, and you want to ensure that you've got a solid narrative that really best positions your organization for any regulatory investigation and/or ultimately any litigation that might stem from the incident.

So in addition to the individual notifications, you're also going to need to determine what, if any government reporting obligations might exist and how and what to disclose in those reports? Your incident response plan is really going to be critical here in lining up vendors ahead of time to assist in any of those notification obligations, whether that's mailing vendors, credit monitoring or call center operation vendors. In summary, understanding and adhering to those specific laws applicable to the jurisdiction in which your organization operates or which may be in scope due to the nature of the information that you all maintain is going to be crucial.

Additionally, careful planning and legal guidance and the preparation of those notification and reports are essential to navigate the complex landscape, the data breach regulations. So Damon, we've now talked about the notification of individuals, notifications of any applicable regulatory or government agencies. Is there anything else in the interim response plan should cover once the notices and reports go out?

Damon Silver:

So if you're dealing with a small breach, a breach that only impacts a small number of people, or if you just get really lucky, it could be the case that you send out the notices and submit the reports and then you can close the book. Nothing further happens, nothing further is required of you. More often though, there's unfortunately another chapter in this journey, which is that in the weeks right after the notices go out, particularly again, if you're sending out a lot of notices, there's likely to be a flood of inquiries from the notice recipients. They're going to want to know more information about what happened. They're going to want to know what the consequences of the incident were for them. They may want to report to you that they think they have been the victim of identity theft. And so as all these notices come in, you want to make sure that you have a well-defined process in place to feel these inquiries quickly because people of course, start to get more and more pissed off if they feel like they're being ignored.

And also, to the point Jason made earlier, consistency in terms of your narrative and in terms of your communications is critical throughout this whole process. You can really create unnecessary trouble for yourself if you have inconsistencies in what you're presenting about the incident and allow people to paint the picture that you're somehow being deceptive. So you want to make sure

that you're responding to requests quickly. You want to make sure that you're responding to them consistently, and you also want to see what type of litigation exposure you might have.

And I mentioned that sometimes you get complaints from individuals that they think they've been victims of identity theft. You want to pay close attention to those and you want, if necessary, collect additional information from those people calling in that might help you assess whether what they're claiming is actually related to your incident or as is sometimes the case, I'm working on one now, you have a whole bunch of people call in say, "I saw this credit card opened up in my name or this medical claim submitted in my name," but it turns out that if you look at the timeline, it couldn't possibly be related to your incident or maybe based on the data elements that were impacted, it couldn't possibly be related to your incident. So you want to start monitoring all of that so you can assess what type of exposure you have and also start thinking about how you would defend yourself.

One other thing you could think about there is in some matters, we will do dark web monitoring, either proactively just to make sure we are aware if any of our data is floating around in the dark web, or certainly after some people have put us on notice that maybe their information is out in the dark web, it's helpful to know what information's out there and what seems to be happening with it.

Another thing that can happen after you submit your reports is that some of the state agencies, which are typically AGs or federal agencies like OCR, which is part of the Department of Health and Human Services, may reach out to you, let you know they've opened an investigation and start asking you questions. And these questions typically will focus on two things. The first is what you'd expect, they want to know about your investigation. They want to know about your response to the incident.

The second though, which sometimes can catch organizations by surprise, is that the agency may want to investigate the adequacy of your pre-incident data security program. They want to know whether you were prepared on the day that that incident happened for what ultimately happened. So the incident response plan we're talking about today is a critical part of that. Having an instant response plan versus not is a very important step in demonstrating that you were prepared. But then there are a lot of other policies and procedures and assessments that you're expected to do based on the nature of your business and your industry and the data you handle. The specifics can vary, but you are expected to have reasonable safeguards in place.

What we found, and obviously if you have a data incident, you can't change what your program look like on the day of the incident, but what we found is that agencies tend to be somewhat forgiving. Even if you didn't really have all your ducks in a row on day one, if between the day of the incident and the day you submit information in response to an investigation, if you use that time to really bulk up your day security program and plug any gaps, that tends to be looked on very kindly by regulators and may be the difference between you getting by with a little slap on the wrist or getting hit with a very stiff minor penalty. On the flip side, obviously if you have an incident and it doesn't seem like you are taking things all that seriously, that can be the type of inaction that invites a much

harsher reaction from the regulator.

So in gearing up for all of these things, sometimes it's all coming to get to the point where you finish your investigation, you send the notices out and the reports out. But as soon as you have a little bit of slack in the system, you do want to start preparing. You want to get yourself ready to make the best showing to a regulator. You want to start thinking about what information you're getting from the notice recipients and making sure that you are as prepared as possible because once the investigations are open or litigation starts, things can start moving very quickly and the theme for this whole episode. But if you are prepared, you're just so much more likely to make good decisions and to act efficiently and make the right moves than if you're trying to do it all on the fly. So Jason, we're very close to the end here. Any final thoughts?

Jason Gavejian:

Yeah, I think it's important to remember that your incident response plan should really be a living document that's going to evolve with your organization's data privacy and security stance. It's got to be regularly reviewed and updated to ensure compliance with any of the new laws or regulations that might come out or even any of the contractual obligations that you as an organization might be agreeing to. Perhaps most importantly, and similar to the fire drill analogy we discussed earlier, it's critical for your organization to practice your incident response plan on a regular basis so that your team's prepared to move quickly if you do experience an incident.

And in the unfortunate event that you suffer a breach, you're going to want to do a postmortem analysis to determine what you could have done better, identify any issues that arose and modify or update your incident response plan as applicable. With that, we've reached the end of today's discussion, but thank you all for listening and don't hesitate to reach out to any of the members of our team if you need help with preparing or reviewing a data incident response plan. Thanks.

Alitia Faccone:

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, Libsyn, 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.

Focused on employment and labor law since 1958, Jackson Lewis P.C.'s 1,000+ attorneys located in major cities nationwide consistently identify and respond to new ways workplace law intersects business. We help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged and stable, and share our clients' goals to emphasize belonging and respect for the contributions of every employee. For more information, visit https://www.jacksonlewis.com.