Podcast

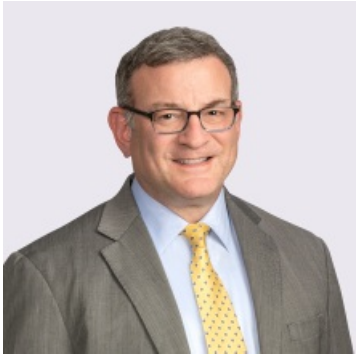
Preparing Your Healthcare Organization for a Data Breach

By Joseph J. Lazzarotti & Michael R. Bertoncini

October 19, 2023

Meet the Authors

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



Michael R. Bertoncini
Principal
(617) 305-1270
Michael.Bertoncini@jacksonlewis.com

Related Services

Healthcare
Healthcare
Privacy, Data and Cybersecurity

Details

October 19, 2023

Hospital systems, physician offices, nursing homes, and other healthcare providers must remain ever vigilant to both safeguard patients protected health information while maintaining compliance with any and all privacy and security regulations. Despite best efforts, cyberattacks are impacting the healthcare industry at an alarming rate. These attacks often lead to data breach class actions.

Jackson Lewis P.C. · Preparing Your Healthcare Organization for a Data Breach

Listen on Soundcloud
Listen on Apple Podcasts
Listen on Spotify
YouTube
LISTEN ON libsyn

Transcript

Alitia Faccone:

Welcome to Jackson Lewis's 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?" Hospital systems, physician offices, nursing homes, and other healthcare providers must remain ever vigilant to both safeguard patients' protected health information while maintaining compliance with any and all security regulations. Despite best efforts, cyber attacks are impacting the healthcare industry at an alarming rate. These attacks often lead to data breach class actions.

On this episode of We get work™, we discuss practical steps healthcare organizations, from single-site medical practices to large healthcare systems, can take to go beyond base-level security to protect their data and their reputation. Our hosts today are Joe Lazzarotti and Michael Bertoncini, principals in the Berkeley Heights and Boston offices of Jackson Lewis. Both are members of the Privacy, Data, and Cybersecurity, and Healthcare groups. Joe co-leads the firm's Privacy, Data, and Cybersecurity practice group, edits the firm's Privacy blog, and is a certified information privacy professional with the International Association

of Privacy Professionals. Joe focuses on the matrix of laws governing the privacy, security, and management of data, as well as the impact and regulation of social media.

A former deputy general counsel of healthcare companies, Mike understands firsthand the competing demands and unique challenges in-house counsel must balance. In his capacity as co-leader of the firm's Healthcare Industry Group, he advises clients on complying with HIPAA and other state and federal privacy and data security laws. Joe and Mike, the question on everyone's mind today is: "How can a healthcare organization protect itself against cyber and ransom attacks, and how does that impact my business?:

Joe Lazzarotti:

Good morning or good afternoon, wherever you are, and thanks for joining us for this next installment of our cybersecurity podcast series. I'm Joe Lazzarotti. I'm a Principal at Jackson Lewis National Law Firm with locations around the US. I'm located here in Berkeley Heights, New Jersey. I founded and currently lead out firm's Privacy, Data, and Cybersecurity Practice Group. I have the pleasure of being joined by my partner, Mike Bertoncini. Mike is a Principal in our Boston office and the co-leader of our Healthcare Industry Group and a member of our Labor and Privacy, Data, and Cybersecurity Practice Group. Mike has a long history in the healthcare industry, serving as in-house counsel for a large health system for several years before joining us, and continuing to guide healthcare entities large and small here at Jackson Lewis. I thought your practical insights, Mike, would be extremely valuable for listeners as they think about the current privacy and cybersecurity landscape, and how they could prioritize their efforts to be prepared for a data breach. So thanks so much for joining, Mike. I appreciate it.

Mike Bertoncini:

My pleasure. Looking forward to it.

Joe Lazzarotti:

So just a few stats, right? According to some reporting by the HIPAA Journal, there are about 395 incidents in the healthcare industry so far this year, resulting in about 60 million records of individuals believed to have been exposed or stolen. The average breach size for 2023 is about 150,000, and over the last 12 months, more than 80 million records have been breached across nearly 700 incidents. So cyber attacks continue to impact the healthcare industry and they are increasingly being followed by data breach class actions. We've seen several vendor data breaches affecting organizations in a big way, including in the healthcare sector. Good example is the recent attacks to secure file transfer providers you may have heard about. You also, Mike work with a lot of healthcare providers, hospitals, nursing homes, physicians offices, et cetera. Give us your sense. What are the challenges that they are facing trying to tackle privacy and security, protecting PHI? What do you see are the big pain points for these kinds of organizations?

Mike Bertoncini:

There's big pain points, really, across the spectrum, and they're not going away. I mean, those statistics you just read are pretty staggering. I mean, data security is on everyone's mind in healthcare, or at least it ought to be. And this is a sector that's seeing constant challenges, right? Everyone in this space is obviously, acutely aware of the need to protect patient information, so there's the ever evolving situation with their electronic medical records. People are constantly looking to update those records. There's a ton of merger and acquisition activity going on in the healthcare space. That means integrating systems. It means upgrading systems. And then, even internally, if you're not doing any mergers or acquisition, you've got interoperability issues, having different sorts of systems speak to one another.

But all of the tech stuff aside, I think, really, there's still no substitute for ongoing employee training, right? I mean, a lot of the literature you see out there says employee error is one of the largest sources and causes of data breaches. So for my money, investing in ongoing employee training is one of the most important things that you can do. The other thing, and some of your initial comments really point to this, you've really got to do your due diligence on your business associate vendors because those vendors ultimately are the source of a lot of the data breaches. And I think in this day and age, that goes to more than just initial due diligence. I think if you've got the wherewithal to do so, you're really talking about doing ongoing auditing of those vendors.

Joe Lazzarotti:

That's really interesting, Mike. I think that makes a lot of sense and I think entities are seeing just that sort of risk playing in their vendors, business associates, and so on. But let me also get at ... in terms of what's the level of urgency? I think some clients I talk to, they're almost exasperated. They don't know where to get started. Some they don't think they're a target, and I'm thinking about it across all industries, and some take it very seriously. Some say, "Well, if it happens, it happens. Que sera, sera, right? So what do you see in the healthcare space in terms of how different types of segments within the healthcare industry, how do they approach this challenge?

Mike Bertoncini:

I think it varies a lot with size and sophistication, right? If you're a single-site medical practice, you frankly, probably don't have the resources necessary to make this your number one priority. So I think everyone in this space starts with the commitment to confidentiality of patient care. But for a smaller organization without a real robust IT function, oftentimes that's just sort of limited to, "I want to make sure I've got base-level security and I've got good physical safeguards." I think as you get out there to bigger, large healthcare systems, they're much more attuned to what's going on out there. And even if you look at some of what's happening with ransomware, a lot of times what you're seeing there are the targets or smaller practices or a single-facility community hospital.

I think, in large part, the measures are unlike a sliding scale based on resources.

And what's unfortunate about that is I think some of the smaller clients are overwhelmed. As you say, they don't even know how to get started, so one way to get started is to call you. But really being able to identify, "What are those steps?" and, "What's going to be reasonable for my scope and my resources?" I think it's not a "one size fits all" solution. However, you're talking about an area where the reputational harm is really, really significant, even if you are a small practitioner. Not to mention, the actual damages to the patients whose data is disclosed. So I think everyone needs to take it seriously. I think some of the smaller organizations probably aren't taking it seriously enough.

Joe Lazzarotti:

Yeah. I guess, Mike, if you look at that and say on the one hand, there's entities that are going to take it very seriously. On the other hand, there's entities that may not have the resources to take it as seriously as they might want to. Either way, both of those entities, breaches could happen. So if you can't maybe prepare as much as you want to prevent a breach and you start saying, "Well, the reality is it's not a matter of if, but when we're going to have a data breach." And so we start thinking about, "Okay, we can do the best we can to prevent it. But when it does happen, we want to be as prepared as possible to weather that storm."

So when you think about your time in-house and working with entities in the healthcare industry, and we do a lot of incident response work, you know that, but what are the things that you'd like to see and where you think could really help to facilitate a healthcare entity's response to a data breach from a practical, operational perspective? I think that might be really helpful for folks to get a sense for, "How do things work and what can I do to improve that response?"

Mike Bertoncini:

Sure. So I think regardless of your size and where you fit on the healthcare continuum, having a break-the-glass kit is essential. So when I was in-house, this was one of the things that would keep me awake at night. "What are we going to do if there's a breach?" But the breach activity that's out there today and the attention it gets from the media is much, much greater than when I was in-house. So the last thing you want to do is find out you've got a breach and be trying to figure out, "Who's my vendor going to be?" and, "Who do I have to contact internally?" and, "What are my next steps?" You don't want to be thinking about a breach for the first time, five minutes after you learned about it. You want to plan in place. And I think unfortunately, this is one of those areas. A lot of times when you're looking at your budgets, the preventive stuff gets left out.

This is a preventive area that you cannot afford to leave out, and I think that's what you lead with when you're having the conversations internally. It's terrible if there's a breach. The best thing you can do if there's a breach is show you have a plan and be active in taking those steps, and be moving immediately on all mitigation fronts, all notice fronts. So to me, that means you've got all the players, internally, who you need. So typically, what's going to be IT, it's going to be risk, it's going to be someone on the medical side, it's going to be someone on the records side. And you've got a plan and it's legal, obviously. You've got a plan about, "What are my breach notifications going to be?" depending on the type of

a breach. You can have the shell of those notifications drafted already. You should have a list of, "Who are the regulators I'm going to have to talk to?" "Who are the law enforcement agencies that I might want to talk to?"

Have all of that stuff gathered in advance. That, I think, is a bare minimum, right? You got to have that plan ready to go, and you have to have an incident command team already identified and ready to go. If you take that one step further, do tabletop exercises. I mean, you do not want to be caught flatfooted. You don't want to be thinking about how will you address a certain problem for the first time when it happens. Have an idea. What are you going to do if you hit with ransomware? Is paying one of the options for you, or is it not? So advanced planning, I think, is a paramount importance and that ties in, again, with the employee training, just ongoing employee training. It's baby steps. Put your building blocks in place and just try to add onto that as best you can.

Joe Lazzarotti:

I'm going to go a little deeper here, Mike, because I think that was great. I think what I find is a lot of times, healthcare entities, and a lot of other industries, they kind of leave this role to the IT person. And certainly, the IT person can be phenomenal and do an excellent job spearheading some of these incidents. But in a healthcare entity, suppose there is a ransomware attack and the systems that help to facilitate care in that attack are also compromised, or there's HR data that's involved, or any number of things that can happen and can be compromised in an incident like this. So if you are thinking about, "All right, I'm going back to my in-house days and I have to pick five people from different divisions or different departments," who do you want in your team to be at that table? And you can't have everybody. It gets too unwieldy. But who do you want to be on that team to help get through this?

Mike Bertoncini:

Right, so you're giving me five.

Joe Lazzarotti:

Well, you could go more if you want. That's okay.

Mike Bertoncini:

Five is probably about right because you can't have too many people in the room. I want IT, I want legal, I want compliance, I want communications, and I want somebody along the lines of your chief clinical officer assessing, "Are we compromising our ability to provide care?" I think that's basically your core team on this stuff. And I want to go back to one thing you said that I omitted. For healthcare providers, because the security of patient information is always paramount. A lot of times the healthcare providers forget, "Oh, there's this whole other scope of data security laws that applies a whole bunch of other information," like HR-related information. So we're always focused on HIPAA. Well, there's a lot more out there than just HIPAA these days, and you've got to be aware of that largely on the state law side.

Joe Lazzarotti:

Yeah. Well, listen. That was great, Mike. Again, I really appreciate that you joined us today. I think this is really an important topic and was really helpful for our listeners who now have a lot to think about, and hopefully some good points to take back to their teams as they evaluate their plans, or maybe that they don't have one and they want to develop one. So I think that's great. And of course, as you mentioned, even if they have a plan, it's probably good to practice that plan and improve their preparedness for an incident. The cyber risks, as we talked about at the outset, show no signs of slowing. Thanks so much again, Mike.

Mike Bertoncini:

My pleasure, Joe.

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.