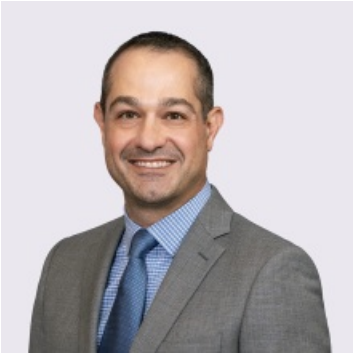
Podcast

Operational Chaos: The Ramifications of a Vendor Data Breach

By Jason C. Gavejian & Stephen T. Paterniti

October 30, 2023

Meet the Authors



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

Stephen T. Paterniti
Principal
617-367-0025
Stephen.Paterniti@jacksonlewis.com

Related Services

Cybersecurity Awareness Audio Guide
Privacy, Data and Cybersecurity

Details

October 30, 2023

Supply chain or third-party vendor disruption can cause operational chaos; specifically, unauthorized access can lead an organization to negligence claims, significant fines, contract disputes, potential lawsuits, loss of revenue, and even reputational harm. Therefore, companies need to secure their data by having robust vendor agreements that address data security and outline their responsibilities in case of a breach.

Jackson Lewis P.C. · Operational Chaos: The Ramifications of a Vendor Data Breach

Listen on Soundcloud
Listen on Spotify
Listen on Apple Podcasts
YouTube

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?

Supply chain or third-party vendor distribution can cause operational chaos. Unauthorized access could lead to negligence claims, significant fines, contract disputes, potential lawsuits, loss of revenue, and even reputational harm. To secure their data, organization should insist on robust vendor agreements that address data security and outline their responsibilities in the event of a breach.

On this episode of We Get Work, the last in our six-part podcast series recorded in conjunction with Cybersecurity Awareness Month, we discuss how businesses can take action to secure their data when working with vendors, the ramifications that a vendor or supply chain breach can have on your business and how to mitigate risk.

Our hosts today are Jason Gavejian and Stephen Paterniti, principals in the Berkeley Heights and

Boston offices of Jackson Lewis. Jason co-leads the privacy data and cybersecurity practice 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.

Steve is an experienced trial attorney and counselor who advises and defends employers on employment issues including discrimination and harassment, wage and hour class and collective actions, restrictive covenants, medical leave, defamation, OSHA, and reductions in force. Jason and Steve, the question on everyone's mind today is, what are the legal and business ramifications of a supply chain or third party-data breach, and how does that impact my organization?

Jason Gavejian:

Thank you all for joining us today. So, Steve, we're here to discuss the potential impact of a supply chain or a third party vendor data breach on a business. Let's just start by briefly discussing what a data breach is. So a breach is a unauthorized access or acquisition of personal information. This often occurs as the result of a business email compromise a ransomware incident, which results in encryption of the business or company systems or data theft, or similar intentional or inadvertent act. It's crucial for businesses to understand the legal ramifications here.

First, data breaches can result in violations of data protection laws, things like the GDPR or the CCPA in California, which certainly could lead to significant fines. Not to mention potential lawsuits from affected customers, employees, partners, patients, or others. Breach can damage a company's reputation and lead to a loss of trust, and that loss of trust then can translate into a loss of potential business opportunities.

If clients are partners, don't believe their data secure, chances are that they might take their business elsewhere. Beyond that, regulatory bodies and industry standards can impose sanctions, revoke certifications, which all can make it more difficult for the business to operate in an effective manner. Lastly, let's not forget about it, the potential intellectual property theft or trade secret exposure during a supply chain or vendor breach, especially as so many entities now are relying on third parties or vendors to store or process their data. This obviously can have significant legal consequences in terms of intellectual property laws and trade secret protection.

Further, there's the security of sensitive employee data. If a data breach results in data theft, it could expose your employees to identity theft issues, fraud and potential privacy violations, which would not only lead to additional legal liabilities, but also significant reputational damage on the financial side, businesses might need to invest in credit monitoring or identity theft protection services for their employees or other impacted individuals to mitigate any of the potential harm that could arise. These expenses obviously can add up very, very quickly. So that's a high-level overview of what a breach is and some of the legal ramifications. But Steve, what about some of

the business issues?

Stephen Paterniti:

Right, so thanks, Jason. So supply chain disruptions due to a breach can cause operational chaos. Legal contracts can also be affected. Businesses may have to deal with breach related liabilities, renegotiations, or even terminations of those contracts. These contracts are a really crucial point. It's important for businesses to have robust vendor agreements in place that address data security and outline responsibilities in case of a breach. These contracts can be pivotal in determining liability. Speaking of liability, companies may need to demonstrate due diligence in vendor selection and management to protect themselves from negligence claims.

On that note, there's also the issue of insurance. Businesses should carefully review their cyber insurance policies to ensure they cover supply chain or vendor breaches. Terms and conditions of these policies can be very complex and they may vary. Understanding what's covered and what isn't is really vital in this arena. Jason, what about notifying affected parties?

Jason Gavejian:

Great point, Steve. Many regulations require prompt notification of data breaches, particularly to state or federal agencies, and failing to do so can result in further or additional legal consequences. Additionally, depending on the nature of the data that's in scope and the data elements that are potentially at risk, that also may be requirements to provide notification to the impact that individuals themselves. As we discussed in some of our earlier podcasts in the series, companies need to have a well-prepared incident response plan that outlines not only the notification procedures, but also containment and mitigation strategies to help them ensure that they're moving through the process quickly and in a timely manner.

This can also trigger investigations into the business's security practices and the steps that they took to prevent such an incident, which can be lengthy and costly. And then there's the issue of public relations and brand reputation. Customers, employees, and partners might lose trust in your business and that experienced a ransomware or similar incident even if it wasn't directly their fault, rebuilding that trust can frankly take years, sometimes decades. So while there's many types of vendor supply chain breaches that can impact your business. For today's discussion, we're going to shift our focus to a specific scenario, a payroll vendor, ransomware incident. So one of your payroll vendors or your only payroll vendor has a ransomware incident that encrypts their system, shuts down their operations, and ultimately prohibits them providing the services that you contract with them to get.

So Steve, how can this impact the businesses that are relying on that vendor for those services?

Stephen Paterniti:

Well, Jason, as you mentioned, there are numerous legal ramifications, but in my view, one area that is rarely discussed is the potential impact on incident at a vendor, especially in today's day

and age, when nearly every organization relies on multiple vendors can have on your business. With respect to a payroll vendor, that's a significant concern, Jason. When a payroll vendor falls victim to ransomware, it can have severe consequences for the businesses that rely on the vendor services. The first and foremost immediate impact is the disruption of payroll processing.

Jason, under the Fair Labor Standards Act, there's no mention of timing of pay, but requirements for when you have to pay employees is covered by state laws, and almost every state has laws requiring you to pay employees in a certain timeframe, often semi-monthly, sometimes two days per month. In my state, Massachusetts, it's generally six days after the last day of the pay period. Of course, there aren't really exceptions under state law to this timing. So the problem is, in case of a ransomware attack that disables the vendor's ability to process payroll, employees still need to be paid pursuant to the timing required under the law. So having a backup plan is crucial. Being prepared with that plan is at least the crucial first step.

Jason Gavejian:

I agree. A plan is a great first step, but let's be honest, in today's day and age, not everybody has a plan. So let's assume that the business isn't prepared with a plan to address an incident like this and its impact on payroll. What are the risks?

Stephen Paterniti:

Right, great question. So we all know employees depend on timely and accurate paychecks. If the vendor can't process payroll due to a ransomware attack, it can lead to financial hardships for employees who aren't getting paid and consequently low morale. Additionally, the affected businesses may face legal and compliance issues, and these can be very significant. They must still adhere to these labor laws and tax regulations even during a ransomware incident. Failure to do so can result in penalties and legal action. Many businesses have to also comply with industry-specific regulations, and payroll data is often subject to stringent security requirements. A ransomware incident can result in regulatory fines and audits.

It's crucial to remember the wage laws don't necessarily contemplate or care about whether a third-party vendor or cyber terrorist is at fault. Employees haven't been paid, and the employer has the obligation to make sure they are paid. Implicit in that is that employers think through a backup plan, as I mentioned before. Moreover, ransomware attack. Delaying pay to employees could cause friction between the company and their employees. Employees might blame the employer for payroll delays or inaccuracies, which can result in employee disputes. They may file complaints with state agencies with the court. It could lead to investigation or audit of the company's practices, pay practice, and otherwise.

The long-term impact of such an incident can be profound. Consider the potential loss of business continuity. If a business can't pay its employees, it could lead to staff turnover and difficulty in attracting new talent.

Jason Gavejian:

Now, Steve, you mentioned legal action. I think any business in today's world is really concerned with lawsuits, or frankly they should be. Can you take us through what a lawsuit in this space might look like?

Stephen Paterniti:

Sure, and these lawsuits, we were seeing more and more of them as we see more and more cyber attacks and ransomware attacks. Business have to deal with potential lawsuits from employees who suffer financial losses due to payroll disruptions. Additionally, they may face regulatory fines or penalties from the state or federal agencies involved for failing to make timely pay. Ransomware attacks likely impact entire workforces.

Class action cases are common in this area, one or a few employees file suit on behalf of everyone impacted. They need to show that all employees suffered a loss due to the same event. But that's easy with ransomware attacks, because it's one event. The class claims aggregate every employee's monetary claims and plaintiff's attorneys get to recover their fees. The exposure in these cases mount very quickly. For example, if you have a thousand employees and an average loss of wages or late pay was a hundred dollars a week and pay is delayed for four weeks, that's $400,000 in potential damages. Some states multiply the damages as a penalty, so these cases can quickly get into seven or even eight figures. Often they settle with a major payoff for the plaintiff's attorneys and modest payments to each employee. So these are very attractive cases for employees.

In addition to wage claims, employers may face privacy claims if confidential employee information was compromised in the attack. That's just a high-level overview of the potential lawsuits that could arise, Jason.

Jason Gavejian:

That's a good point. So Steve, if an employer's payroll vendor suffers a ransomware attack and now the vendor's not able to provide payroll services and the employer's not able to actually get their employees paid, what are some other ways that the business can address this issue?

Stephen Paterniti:

So I mentioned before backup plans. Capturing hours can be done using old-fashioned methods. You could use paper records, punch clocks, emails from employees to their managers with hours worked that week. There are apps on smartphones that have been developed for capturing and reporting time. Figuring out how to get from capturing accurate hours to paying the employees can be a challenge and nearly impossible to do in a very short timeframe when the emergency hits. Some employers with financial means in these situations have just doubled every employee's pay from the prior pay period to cover its basis. But frankly, none of these are perfect solutions because typically, you're dealing in a varied condensed time period and the problems and the

logistics are immense.

Jason Gavejian:

So litigation's a big concern. But what about dealing with the payroll vendor themselves?

Stephen Paterniti:

Right. The situation with the payroll vendor with a ransomware attack often leads to contractual disputes with the payroll vendor itself, because from the employer's perspective, they did nothing wrong. It was the payroll vendor who had some sort of security breach. If the vendor fails to meet their service-level agreements due to the incident, businesses may seek compensation or even terminate the contract. With regard to these contracts, the issue indemnification is critical to focus on. Businesses need to review their contracts with the payroll vendor to understand the vendor's liability in the event of a ransomware incident or other event that prevents them from providing services.

Jason, any closing thoughts?

Jason Gavejian:

Yeah, thanks Steve. So in summary, data breaches stemming from a supply chain or vendor vulnerability can lead to regulatory fines, lawsuits, a loss of trust, a reputation, contract disputes, insurance complications, liability issues, notification requirements, and even potential intellectual property theft. A payroll vendor ransomware incident has potential long-term impacts, including business continuity issues, regulatory challenges, in addition to potential lawsuits including class actions. These incidents can have a cascading effect on the businesses and their relationship with their employees, their customers, and certainly, the payroll vendor themselves.

It's really a multifaceted challenges. Businesses should be really proactive in assessing and mitigating these risks. And of course, they should be seeking out expert legal counsel to navigate these complex waters. As we've said throughout this entire podcast series, it's not a matter of if a breach will happen, but when, and being prepared with a legally sound compliance program is really the best process for you to have a strong defense, and that really includes ensuring that your business interruption or your incident response plan accounts for a potential supply chain or vendor, data breach or data incident.

Thank you all for joining today, and please don't hesitate to reach out to any of my Jackson Lewis colleagues or myself should you have any questions or concerns in this area. 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.