Articles + Publications | October 23, 2024

6 Tips for Cos. Facing Service Provider Cyber Incidents

WRITTEN BY

Kaitlin J. Clemens | Sadia Mirza | Ronald Raether, Jr. | Karla Ballesteros

Published in Law360 on October 23, 2024.

It is no secret that ransomware dominates headlines, and cybersecurity incidents have become part of our everyday language. However, the criminal "business model" behind ransomware keeps evolving.

Current data protection laws and regulations do not fully address the complexities of targeted attacks on third-party service providers who may hold data for thousands of businesses and millions of consumers. Additionally, most incident response plans do not account for situations where the investigation may be out of the business's control.

Despite these challenges, businesses continue to be inundated with headlines and notifications from third-party service providers about these "common incidents," which can affect hundreds, if not thousands, of businesses.

The CDK Global incident is a prime example. CDK is a software vendor that provides applications for the automotive industry, particularly for car dealerships to manage vehicle sales, financing and daily operations. On June 18, CDK announced it suffered a ransomware attack taking many of its core systems offline, affecting business operations for dealerships across the country.

CDK issued a statement to its dealers with an update on the security incident on July 30, noting that there was no determination if any personally identifiable information was affected.[1]

When businesses learn that their third-party service provider has been affected by a cybersecurity incident, they are left to wonder: What now? Was our information compromised? Are our systems safe? How do we continue business operations? Are our losses covered?

The reality is, during third-party service provider incidents, businesses are not usually the ones in the driver's seat. However, they need to focus on what they can control before, during and immediately after an incident and plan for the day they are taking that passenger ride.

Below are some steps businesses should consider for a smoother ride.

1. Ensure your environment is secure.

When a business receives notice of a cyber incident affecting a service provider, the first priority should be securing its systems and environment.

This may involve hiring a forensic investigation firm to thoroughly check the systems. Often, these firms are already assisting other businesses in similar situations and can share valuable insights. However, a preliminary check by the business's own team might reveal that a full forensic investigation is not necessary.

The main focus should be on identifying any integration or connection between the service provider's system and the business's environment. This includes confirming whether any credentials used in the business environment may have been compromised due to the service provider's incident, or if there is a virtual private network tunnel between the service provider and the business's systems.

For instance, in the CDK incident, for some customers there was an "always-on" VPN connection between CDK's data centers and car dealerships, allowing local dealership applications to interface with the CDK platform. A potential concern was whether the threat actor could use this VPN connection to access the internal networks of car dealerships. Even if the ransomware wasn't intended to spread, it could still do so if the mechanisms allowed it.

To protect against a secondary attack, it is crucial for internal teams to quickly shut down any integration between systems and rotate credentials. It also should reassess segmentation rules and limiting any lateral movement from a service provider compromise. If there are still concerns about the security of the environment, a forensic investigation firm can provide additional assurance that the systems are secure.

2. Consider business continuity options.

After securing the business's systems, maintaining operational continuity should be the next priority.

Businesses should explore various options to mitigate potential disruptions. This could include considering alternate service providers — even if only temporarily — to ensure continuous operations. In some cases, reverting to manual processes, like using pen and paper to document transactions, may be necessary.

For example, during the CDK incident, many car dealerships resorted to manual methods to complete normal purchase and service transactions. They also had to devise alternative payroll processes to ensure employees were paid on time.

This situation highlighted the importance of having a robust business continuity plan in place. Such a plan might include using previous payroll data and reconciling later or establishing alternative purchase and service processes to maintain operations during a disruption.

To prepare for potential business disruptions resulting from service provider incidents, businesses should take the following steps.

Identify critical service providers.

Determine which service providers are essential to business operations and functions.

Create backup plans.

Develop backup plans for key processes, such as payroll, customer service and supply chain management. This might involve setting up agreements with alternate service providers or having manual processes ready to deploy.

Train employees.

Ensure that employees are trained on the business continuity plan and know how to execute manual processes if necessary. Regular drills and simulations can help prepare the team for real-world scenarios.

3. Hire a forensic accountant.

Waiting for updates from a service provider on the restoration of services can be one of the most frustrating aspects of third-party service provider incidents.

The service provider may have notified the business of the incident due to contractual obligations or reputational considerations, but they might not be able to provide a firm deadline for restoring services. This leaves the business in a holding pattern, potentially losing money due to the service disruption without a clear timeline for returning to normal operations.

In such situations, businesses should consider bringing in a forensic accountant to help determine and document any potential losses. This step is crucial if the business plans to file an insurance claim. A forensic accountant can provide guidance on the impact, identify overlooked areas of loss, and assist with tracking losses as they occur, ensuring accurate records for substantiating claims.

Additionally, having a forensic accountant involved early can offer other benefits. They can help identify areas to mitigate further losses, advise on cost-saving measures during downtime, and assist in communicating the financial effect to stakeholders, including investors.

Failing to track these data points early on can make it difficult to recreate them later, potentially resulting in lost money. By tracking losses in real time, businesses can ensure they have accurate records to support any insurance claims and better understand the financial effect of the incident.

4. Review legal notification obligations and stay updated on regulatory developments.

If a service provider handles personal information on behalf of a business, the business may have legal notification obligations to individuals and regulators due to the incident.

The law distinguishes between data owners, who collect information directly from individuals and determines the purposes and means of processing that information, and service providers, who process or store information on

behalf of data owners. Generally, data owners are required to notify individuals and regulators of any data breaches, whereas service providers are only required to notify the data owner and provide sufficient information so that the data owner can, in turn, comply with its notification obligations.

In simpler times, this process was straightforward. It typically involved the service provider giving the affected business a list of affected individuals, the affected data elements for each individual, and the individual's address, if available. This information allowed the business to determine its notification obligations and provide notifications to individuals and regulators accordingly.

However, as businesses have become more reliant on service providers and the volume of data managed by both has increased, determining an appropriate notification strategy has become more complex. This complexity is especially pronounced when a common incident occurs, affecting hundreds or thousands of businesses simultaneously. Adhering strictly to the law, regulators and individuals may be inundated with notifications of the same incident from various businesses, leading to inefficiencies and potentially increasing consumer panic.

Although data protection statutes and regulations continue to place the responsibility on the data owner to provide notifications, regulators are beginning to acknowledge the complexity involved.

For instance, it was reported that CDK and the National Automobile Dealers Association came to an agreement with the Federal Trade Commission that if CDK's internal investigation determines that notice to the FTC is required, CDK will issue an omnibus notice covering the incident. This agreement purportedly would relieve each CDK dealer of the obligation to independently notify the FTC.[2]

Staying informed about updates from your service provider, such as the FTC update from CDK, should guide the business's notification strategy. This approach ensures the business complies with regulations while aligning with the actions of thousands of other affected businesses, avoiding unnecessary attention.

Organizations can also prepare for service provider incidents by including this scenario in a tabletop exercise, wherein the organization enacts a service provider cybersecurity incident and what they would do in response. This can help organizations to prepare a protocol or playbook for service provider incidents and outline the specific legal notification obligations that will be at issue.

This is especially important for regulatory reporting obligations with tight deadlines, such as the U.S. Securities and Exchange Commission's cybersecurity reporting obligations for publicly traded companies.

5. Extend some grace to your service provider.

Dealing with a service provider during a cyberattack can be challenging, but it is important to extend some grace. Cyberattacks are increasingly common, and thorough investigations and recovery efforts take time.

While the service provider is the victim of the attack, your business's reputation is also at stake. The priority should be to ensure that only accurate information is shared with relevant stakeholders, including details about the nature and scope of the incident.

Allowing the service provider sufficient time to conduct a thorough investigation is crucial, as their findings will inform your next steps, strategy and potential liability. Rushing this process could lead to inaccurate information, undermining the credibility of the investigation and your ability to navigate it appropriately.

However, allowing time for the investigation does not mean businesses should remain passive.

Proactively reaching out to the service provider and establishing a regular schedule for updates is key. If the service provider has engaged legal counsel, the business may consider using its own counsel for the initial outreach to facilitate communication.

Remember, it is common for service providers' support teams to become overwhelmed with inquiries following a cybersecurity incident, and outreach from businesses can easily be overlooked or lost in the shuffle. Therefore, businesses should assess the most appropriate form of outreach based on the nature of the business relationship and determine which method will be most effective in obtaining a response from the service provider.

6. Find the path forward after a common incident.

Before an incident occurs, businesses should include provisions in vendor agreements that clearly outline the service provider's responsibilities in the event of a cybersecurity incident, including the specific timing for reporting such incidents.

By establishing a clear reporting time frame and detailing what information must be included, organizations can make more informed decisions about their own reporting obligations. This can help determine whether to file a claim with their cyberinsurance carrier or report the incident to regulators with strict deadlines, such as the SEC, the Office for Civil Rights, and the like. This approach can minimize uncertainty and establish expectations for reporting updates and sharing information.

Following the incident, businesses should prioritize securing their systems, maintaining operations, and accurately tracking and documenting losses. After allowing the service provider time to respond, businesses should regroup with the service provider to discuss the service provider's communication plan and strategy, as well as any resources the service provider will make available, including those related to notifications and regulatory compliance.

These issues can also be discussed in advance, which will inherently strengthen the partnership between businesses and their service providers. This proactive approach also serves as a reminder that, ultimately, it is not a matter of business versus service provider; rather, they share a common adversary — the threat actor. By working together effectively, both parties can manage the response more efficiently, leading to favorable outcomes for everyone involved.

---

[1] https://complyauto.com/cdk-issues-update-on-security-incident/.

[2] https://www.nada.org/nada/nada-headlines/nada-chairman-gary-gilchrist-provides-update-top-issues#:~:text=While%20dealers%20still%20must%20contend,FTC%20related%20to%20this%20matter.

RELATED INDUSTRIES + PRACTICES

- Incidents + Investigations
- Privacy + Cyber