beazley

Article

Your vendor has been breached: Now what?

June 22, 2023

If your organization discovers that your data has been compromised because one of your vendors has experienced a breach, you will face a unique – and complicated, set of challenges.

Vendor breach – why it’s complicated

If your organization discovers that your data has been compromised because one of your vendors has experienced a breach, you will face a unique set of challenges. All the usual issues involved in a response - conducting a forensic investigation, determining notification obligations, notifying in a way that preserves customer relationships - become much more complicated when the breach has occurred at the vendor.

Taking control at the outset is critical. That's true when you enjoy a strong relationship with the vendor, but even more so if it's a former vendor or if the relationship has become strained. As the data owner, you must learn the details of the breach and be able to identify and notify affected individuals in order to fulfill legal requirements.

What to do immediately

Organizations typically become aware of these incidents when they are notified by the vendor or the incident is disclosed publicly. We recommend that once your vendor informs you of a potential or actual breach affecting your data or you learn of it otherwise, you notify Cyber Services. Having helped our insureds through more than 2,000 vendor-caused incidents, Cyber Services can help explain what issues commonly arise and how they affect the timeline for investigation and response.

Understanding what has happened during a vendor breach can be challenging, particularly early on. Because we frequently receive

multiple notifications related to the same vendor breach, we're able to help our insureds streamline their response, by coordinating services from data breach counsel and forensics providers who are already working on the incident and have the latest information about what the cybercriminals did and what data may or may not have been exposed.

Controlling the situation

One significant complication in a vendor incident is that you may not control the forensic investigation. In fact, unless your contract with your vendor requires they notify you within a certain timeframe, they may already have spent significant time on the investigation, eating into regulatory deadlines for notification to affected individuals. Experienced incident response counsel, particularly if already engaged in the incident with others, can help you understand what information you need to get from the vendor to determine whether you have notification obligations. Working with specialists already knowledgeable about the incident also helps you benefit from any developing forensic analysis.

Understanding legal requirements

Understanding whether your organization or the vendor has the obligation to notify affected individuals, if notification is required, is another challenge in vendor-caused incidents. State breach laws typically place the obligation to notify on the data owner or licensor, which would usually be your organization rather than the vendor. Depending on your contract with your vendor, however, the vendor may be obligated to assist in or undertake the notification process. For organizations subject to HIPAA, having an appropriate business associate agreement (BAA) in place is essential. In one case, following a report of patient information exposed on the website of a billing provider, the investigation revealed that the covered entity had no BAA with the vendor, leading to a $500,000 payment to settle potential violations of the HIPAA Privacy and Security Rules.

Finally, the actual notification process poses challenges. In some cases, the vendor may merely provide a list of affected individuals, leaving your organization in control, and in that case Cyber Services would work with you to coordinate notification services, a call center, and credit monitoring if required. More often, in our experience, vendors are willing to undertake notification as a matter of customer service. But if your customers are affected, you want to make sure that you're involved in the process to help preserve goodwill and prevent reputational damage, make sure notifications meet your legal obligations, and avoid pitfalls that may lead to regulatory investigation or litigation. Experienced data breach counsel will help you work through these issues to achieve the best outcome for your organization.

Managing vendor risk

Of course, vetting providers and making sure you have in place appropriate contractual protections are two important steps you can take to help protect your organization. Beazley cyber policyholders can find additional guidance on our risk management site:

Cybercrime Spotlight: Uncovering Supply Chain Security Risks

Reducing Your Risk: Cloud Computing

Privacy Builder Module 6: Vendor Management

DISCLAIMER

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.

The descriptions contained in this communication are for preliminary informational purposes only. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., and is available on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd’s. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: OG55497).

beazley