The Ultimate Guide to Vendor Data Breach Response

This paper was authored by Corvus's VP of Smart Breach Response Lauren Winchester in collaboration with Dominic Paluzzi, Co-Chair of the Data Privacy and Cybersecurity practice at the law firm McDonald Hopkins.

The Ultimate Guide to Vendor Data Breach Response

Cyber insurance brokers help their clients plan for what happens when they experience a data breach or ransomware incident. Something often overlooked is how that plan may change when the breach is at a vendor and the investigation is outside of their control.

Most organizations are in the midst of a decade-old shift to deeper integration with managed service providers, software-as-a-service tools, and other cloud-based software solutions. Having worked with thousands of brokers and policyholders, we've observed an unspoken assumption that these vendors, with their highly advanced products, are also paragons of cybersecurity. That's a misplaced assumption for three reasons.

1. **The bigger and more complex an organization, generally the harder it is to keep safe.** Vendors may have excellent security teams and practices, but face a sisyphean task given their scale.

2. The adversarial question. **These companies may be at greater risk because criminals see them as a rich target** -- if they can infiltrate the vendor, they can potentially extend their attack to hundreds or thousands of customer organizations.

3. **Some providers have an air of invincibility about their exposure,** likely for the same reason their customers instinctively trust them. A survey by Coveware shows a large disconnect between what MSPs believe to be the cost and consequences of an attack, and what they are in reality.

Supporting this note of warning, some relevant data has emerged of late. Attacks on IT managed service providers (MSPs) increased 185% in 2019 according to Crypsis, and MSPs are being called a "worrying new frontier" for ransomware. In a survey of 600 companies, 44% reported experiencing a vendor-caused breach. And in May 2020, a ransomware attack on Blackbaud, a widely used cloud services provider for nonprofits, had broad implications for thousands of organizations.

These worrying trends and real-world situations have resurfaced questions among brokers and their clients about what companies should do when their vendor is targeted. **This whitepaper aims to help insurance brokers better understand incident response best practices when their clients are impacted by a third party cyber incident.** We'll cover what your clients should expect if their vendor is breached, the first steps they must take to mitigate damage, and the questions they need to ask of the vendor to get the information they need.

My client just got an email from a vendor saying they are experiencing an incident. What do we do first?

The first step for any organization is to take a step back and breathe. This might feel like uncharted waters if they haven't experienced it before, but they should understand that there are well-defined steps to take based on many, many thousands of incidents. Being a cyber insurance policyholder, they likely have the help of cybersecurity experts (not to mention their broker) at their disposal.

If their leadership has planned for an incident, they can turn to their incident response plan (IRP) and convene any necessary members of the incident response team. Within the IT department, the focus should be on making sure their environment is secure and not somehow at risk.

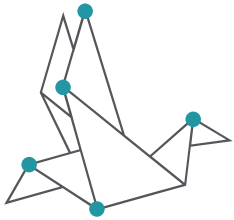
Other important initial steps to take include notifying their broker and cyber liability carrier, and retaining experienced privacy counsel. Privacy counsel that have a robust incident response practice may very well be assisting other clients impacted by the same vendor, which allows for an efficiency gain and gives that law firm more leverage with the vendor, hopefully increasing responsiveness.

Finally, someone within the organization should pull up the contract with the impacted vendor to start understanding rights and liabilities. Provisions to pay particular attention to include a breach notification provision (if it exists), indemnification provision and confidentiality provision.

Who do we have to tell about this, and when?

Companies will be subject to a patchwork of laws and regulations that can apply depending on the type of data and location of the data subjects. They should find out right away what kinds of data are potentially involved, so the organization and their counsel can start to analyze reporting requirements.

Each state in the U.S. has its own data breach notification statute, and certain industries will also have specific laws or regulations for data breach notification: HIPAA for healthcare, FERPA for education[1], NY DFS for financial institutions doing business in NY, GLBA for financial institutions[2], to name a few. If applicable, other countries have laws or regulations requiring data breach notification, most notably the GDPR in Europe and PIPEDA in Canada. Each of these laws or regulations will have their own obligations with respect to notification, regulatory notices, what data is protected, the time within which an organization must give notice and other nuances.



1 FERPA does not actually require notification to individuals - just that the institution maintain a record of the disclosure. That said, other breach notification statutes may apply depending on the type of student information compromised.

2 The GLBA does not have an explicit data breach notification requirement, but the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice does.

What information do we need to get from the vendor?

It's important to ask the right questions of the vendor as quickly as possible once learning of the incident. This list shows where they can start. Feel free to share these questions with your clients to have on hand.

What happened and how?

Getting a basic sense of the scope and type of incident will help guide response and resource allocation.

Has the compromise impacted our system, and if not, how have you come to this conclusion?

The vendor may report that your business has not been affected, and of course that would be welcome news. But it's important to probe further. There's a good chance that the vendor has not yet completed a full investigation, and you don't want a nasty surprise later if the vendor was premature in their conclusion.

How far into the investigation is the vendor, and which incident response firms are supporting their efforts?

The hope here is that they've not only engaged legal and forensics, but they've chosen well known firms that regularly conduct incident response investigations. If the firms are not well known for incident response, the concern is that their lack of experience will lead to a slower response or poor advice to the vendor.

Is there a forensic report, and can we have access to it?

If the vendor sends a copy of their forensics report, that will be very helpful to the organization's own investigation and response, but do not be surprised the vendor refuses to produce the report. They may be trying to assert the attorney client privilege. If that's the case, ask if they can share a summary.

If ransomware - what variant? Did they pay the ransom or do they have backups? Do they have endpoint monitoring in place to make sure the incident is contained?

The strains of ransomware in use by criminals today are capable of leaping across an organization's IT network remarkably easily, as well as hiding out unnoticed, lying in wait to strike again. Don't let the vendor's sloppy response practices become a second headache later.

What data of ours has been compromised, and if so, when will we be provided with a list? Will the vendor be paying for notification, call center and credit monitoring if we are required by law to notify affected individuals?

The vendor is likely required by the breach notification statutes or regulations in play to tell you what data was compromised and give you a list of impacted individuals. But often vendor contracts are silent regarding data breaches (or unfavorable to the organization), so the vendor may not be obligated to take on

the effort and costs of notification. Ask the vendor early on (in writing) if they will pay for notification if required.

How many of the vendor's customers are impacted?

It's important to try and get a sense of how big the scope is, in order to gauge where you fall within the vendor's priorities. If the company has hundreds or thousands of affected customers who are likely asking the same questions you are, unfortunately that means gearing up for a battle for their attention.

Does the vendor have cyber insurance?

Hopefully the vendor has cyber insurance so that they have the resources to do a proper investigation and response. A lack of cyber insurance may signal that the response will be underfunded and therefore less thorough.

Will you pay for our legal fees if we hire a lawyer to help us with evaluating our breach notification obligations?

Some vendors will agree to pay for reasonable legal fees of their customers in an effort to retain their business. It's worth asking the vendor early on, particularly if you are an important customer.

What is your plan for security enhancements to try and prevent this from happening again?

The organization's faith in its vendor's security is shaken, so future decisions around whether to continue the relationship with the vendor should depend on how satisfactorily the vendor answers this question.

If there are affected individuals, who's responsible for notifying them - us or the vendor?

There is a big misconception that the entity holding the data will be responsible for notification. What the data breach notification laws ask is who owns the data. At the end of the day, the data owner has the notification obligation to affected individuals. The vendor is required to notify the data owner and provide information about what happened and what data was impacted.

That said, organizations can (and whenever possible should) look to contract around the laws by either requiring the vendor to give notice or requiring the vendor to indemnify the organization for the costs of responding to a breach of the vendor's systems. But even if a vendor agrees (by contract or otherwise) to handle the notification, the organization must still ensure the vendor is meeting their notice obligations as regulators could open an investigation.

Ok, we know what we have to do. What are other challenges to look out for when dealing with a vendor incident?

The biggest challenge will be overcoming a lack of control over the investigation and its pace. Often, the organization won't be privy to the forensics and facts unless the vendor chooses to disclose them. They are very much at the mercy of the vendor for answers, which is a frustrating position to be in. With this lack of control come timeline challenges -- vendors tend to wait to notify their customers until they have something substantial to report, and this can impact an organization's third party exposure down the line. It is common in a vendor breach that individuals do not receive notice until well after the required notice timelines. In addition, contracts are typically not favorable to the customers. Often liability is limited, indemnity is limited, the contract is silent as to who handles breach notification (leaving it to the data owner).

"The more impacted entities and disparate approaches, the harder it is to get the client to take a measured approach."

Finally, every downstream customer of the vendor has the potential to react and respond differently. This leads to inconsistent approaches to notice that can pressure organizations to go against an experienced counsel's advice because "other entities are doing it." The more impacted entities and disparate approaches, the harder it is to get the client to take a measured approach.

What does "good" look like?

Ideally, the vendor owned the breach from A to Z! They were transparent with the forensics investigation and findings, allowing their customers' counsel enough insight to give legal advice on notification obligations to the customer. The vendor hired experienced counsel and forensics with a consistent and proven track record in incident response. They identify the exact information compromised for each affected individual, and offer to handle notification to individuals and regulators to ensure a consistent message. They offer a dedicated call center and credit monitoring if appropriate. And finally, the vendor provides adequate assurances that they've contained the incident and will continue to monitor so as to prevent this from occurring again in the future.

Want to learn more about Breach Response at Corvus? Contact us at services@corvusinsurance.com or get caught up with the resources below:

Breach Response & Risk Mitigation Services:

- [PDF] Corvus Smart Cyber Insurance Breach Response & Claims Handling
- [PDF] Corvus Black: Premier Risk Management from Corvus

Insights from the Breach Response Team:

- [Blog] Breach response during a pandemic: what brokers and their clients can expect
- [Blog] A recent legal decision could change how clients handle breach response. Here's how.
- [Webinar] BEC: (Unfortunately) Easy as 1, 2, 3

CORVUS

McDonald Hopkins
Celebrating 90 Years

About Corvus

Corvus is reimagining commercial insurance for a digital world by making insurance smarter, companies safer, and brokers more successful. Corvus empowers brokers and policyholders with actionable insights to mitigate complex risks and reduce losses through the CrowBar® digital platform, smart insurance products, and premier risk management services. Corvus is the world's largest specialty commercial InsurTech company.

Founded in 2017 by a team of veteran entrepreneurs from the insurance and technology industries, Corvus is backed by Telstra Ventures, Obvious Ventures, MTech Capital, Bain Capital Ventures, Hudson Structured Capital Management, and .406 Ventures. The company is headquartered in Boston, Massachusetts, and has offices across the U.S.