PUBLICATION

Vendor Relations – Your Best Friends Really Can Hurt You

Authors: Samuel Lanier Felker
May 09, 2017

Baker Donelson's Data Protection, Privacy and Cybersecurity attorneys are pleased to continue a series of client alerts that address significant cyber-threats to your business and discuss ways you can protect your business with thoughtful and timely planning before an emergency arises. Proper planning includes recognition of the threats, assessment of the risk, and then examination of the facts and tools at your disposal to mitigate the risks. The series will address your options, from adopting appropriate IT policies and procedures to acquiring contractual indemnity and insurance for specific loss risks. When there is a recommended technical solution available, we will consult with leading expert vendors and provide their input. We often hear that in today's tech environment, it's not a matter of whether you will be hacked or attacked, but when; therefore, we want to help you be well prepared for future challenges.

Our series will help you get ahead of the game. We offer guidance on shopping for cybersecurity insurance; protecting your business from DDoS attacks and ransomware; establishing a smart data management plan; and evaluating vendor relationships.

Vendor Relations – Your Best Friends Really Can Hurt You

Your team is only as strong as its weakest link. This platitude may be overused and cliché, but within the data privacy and cybersecurity space, the expression is more of a warning and must be taken seriously as essential advice. Vendors and third-party service providers create a unique challenge to organizations that are looking to streamline the services offered to their customers while implementing controls and safeguards to protect their customer's data.

There should be a balancing act taking place within each vendor contract, where your organization should be aiming to find the sweet spot of vendor access to your organization's and your customer's data, which allows a vendor to provide the requested service without risking your customer's privacy. Too often an organization will permit a vendor untethered access to their internal systems and/or customer data while also placing insufficient controls on the vendor's activity. This is a recipe for disaster.

The Tenth Annual Verizon Data Breach Investigations Report addresses this risk by stating, "We recommend all businesses, small and large, ask the right questions to any third-party management vendors about their security practices." The Report underscores the importance of this advice by pointing out the frequency of hacking through vendor access: "Following the same trend as last year, 95% of breaches featuring the use of stolen credentials leveraged vendor remote access to hack into their customer's point of sale environments."

So what are the best practices that can be implemented in order to limit your risk?

Prior to Onboarding

When evaluating vendors and third-parties, you should have a robust due diligence process where your vendors' data security policies, procedures and controls are thoroughly reviewed. All vendor standards should meet or exceed standards implemented by your organization. In the event of a breach through a vendor, you want to be able to show that your organization was not negligent when it came to onboarding the vendor and did not unknowingly allow for a weak spot in the organization's data protection plan. This is especially true if, within your industry, you are promoting your organization's data protection ability.

When negotiating each vendor contract be sure that you provide for data security reporting standards, which will include a timely notification of any breach, attempted breach or other data security incident. Include non-disclosure clauses covering any of your organization's and/or your customer's private information. Your agreements should also provide for the right to require changes to standards as external and internal environments change, as this space is evolving on an almost daily basis. It is a mistake to have contacts that call for or define a static security standard that cannot evolve with the best practices implemented within your industry. Finally, your contacts should provide that your organization, or an auditor which you choose, has access to your vendors' systems.

After these controls are in place, it is also important to have a thorough understanding of what your vendor is doing with the information you permit the vendor to access. For example, as behavioral advertising continues to grow, many marketing departments engage vendors to assist and are unaware of what the vendors are doing with aggregated data that is collected by the vendors at the organization's request. This is vital information that you should be aware of and possibly disclosing to your customers, depending on your industry and privacy policies.

Oversight Once Engaged

Proper vendor oversight does not end after onboarding is complete. You will need to provide for continued oversight that ensures your vendors are honoring their commitments and living up to the standards and processes laid out in your vendor agreements. Your organization should have controls in place to monitor if data privacy and cybersecurity risks are being appropriately identified, measured, mitigated, monitored and reported to your organization on a consistent basis. These controls should be deployed on a routine basis as frequently as possible.

Vendor data privacy and cybersecurity risks are often only thought of when looking at issues surrounding the Internet of Things (IoT) issues, where certain equipment and vendor-provided devices are creating network and/or data access points and/or FinTech issues, where lenders are entering into vendor agreements to provide services that traditionally were unavailable to borrowers. However, it is important to note that ***all*** vendors your organization is employing must be subject to the aforementioned best practices.

As was heavily reported, the hackers in the Target breach of 2013 gained access through Target's HVAC vendors, as these vendors had remote access to Target's network to perform maintenance issues. This is a perfect example that it's not just the vendor's intended use that poses risk; it's the access that can be gained through the vendor whether said access was intentionally or mistakenly granted. For this reason, you should always be asking what access will the vendor need and is this the most limited access needed to accomplish the tasks at hand? It may be costly to carve out and limit each vendor's access, but that cost will be eclipsed by the costs associated with a breach that could have been avoided.

The best practices outlined above are a good start to limit your exposure to hacking through vendor access. These tips will also mitigate your litigation exposure if a breach were to occur through your vendor, by providing an argument that your organization was diligent in attempts to safeguard all customer data. In addition, depending on what industry you are in, there are multiple regulatory risks and privacy issues that need to be addressed and guarded against when allowing vendors access to your internal data.

If you have any questions or concerns about your organizations data privacy and cybersecurity protocols or industry specific questions, please reach out to any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team and we will be happy to assist.