PUBLICATION

Best Practices for Protecting Operations from Vendor's Cyber Incidents

Authors: Dandridge S. Parks, Layna S. Cook Rush
October 07, 2024

In the aftermath of a vendor's hack that crippled an industry, ensure your business is up to date on best practices for mitigating the risks of third-party cyber incidents.

Many businesses struggle to adequately consider the risk to their operations if a third-party vendor experiences a cybersecurity incident. The sudden lockout or shutdown of a critical vendor can cripple business operations. The recent Change Healthcare breach nearly gridlocked the U.S. health care sector and should serve as a wake-up call for businesses to carefully consider their vulnerability to vendor cybersecurity incidents. Vendor risk mitigation, business continuity planning, and contractual protections are now critical considerations for companies, particularly those with a large suite of vendors.

Why a Vendor's Vulnerabilities Are a Bigger Problem Than You Think:

Software as a Service (SaaS) applications are now used enterprise-wide, from operations to human resources to payment processing. The number of SaaS applications used by the average business has been growing steadily for the last decade. At the same time, the number of cybersecurity incidents and data breaches has grown exponentially. As AI tools enable more complex and convincing attacks by criminals, there is little reason to expect that trend to reverse. As the number of vendors and attacks grow concurrently, it seems inevitable that a critical vendor for most organizations will suffer a breach in the foreseeable future.

In the spring of 2024, Change Healthcare (a subsidiary of UnitedHealth Group) suffered a cyberattack that was "the most significant and consequential incident of its kind against the U.S. health care system in history," according to American Hospital Association President Rick Pollack. The ALPHV/BlackCat ransomware group claimed responsibility for the attack; they were able to steal up to four terabytes of personal information, records, and payment details. More significantly, this attack spurred devastating financial consequences for the health sector, as many physicians relied on Change Healthcare to process claims and claim payments. A survey from the American Medical Association (AMA) found that 80 percent of practices lost revenue from the attack and that small practices were particularly hard hit. Alongside general "tremendous financial strain," AMA President Jesse Ehrenfeld noted that "these survey data show, in stark terms, that practices will close because of this incident."

The Change Healthcare breach offers several lessons: (1) any vendor can fail unexpectedly, even those that are large, ubiquitous, or sophisticated; (2) while the concern over a vendor's breach is often that it will result in hacker's access to your systems, there are also significant operational risks to a vendor breach; and (3) failing to plan for those operational risks can have significant consequences.

It is, however, still a concern that a vendor's cyber incident will result in unauthorized access to their customers' systems. SolarWinds is still squaring off with the SEC over the 2020 breach that resulted in Russian hackers gaining access to the U.S. Department of Homeland Security, among others. A recent ruling found that SolarWinds grossly misstated its cybersecurity protections, allowing the SEC to take the company to trial on the issue. Other vendors may also overstate their own cybersecurity compliance.

Best Practices for Business Continuity Planning and Vendor Management

Business continuity planning, vendor management, and strong contractual protections are imperative to keeping your business operations functioning through a vendor's breach. As a company incorporates vendor-procured software throughout its organization, it is critical to consider vendor cybersecurity risks holistically. The MOVEit breach of 2023 highlights how risk exists even for mundane software, like a file transfer service.

Undertaking Business Continuity Planning (BCP) on the front end is a good way to avoid the financial and reputational damage associated with vendor cybersecurity incidents. Some of the BCP best practices to ensure that your organization can navigate shutdowns and disruptions are to:

- Know your critical functions and the vendors associated with each function. Consider that often-overlooked technology, like a file transfer system or payment processing software, can gridlock your company if it goes offline;
- Create contingencies, backups, and alternative solutions to each critical function. Consider using multiple vendors for the same service to prevent a chokehold in the event of a breach;
- Consider the extent to which each vendor is integrated into your organization;
- Similarly, consider which vendors are obsolete or unused. Companies often maintain vendor relationships despite not using the service, which wastes money and creates unnecessary cybersecurity risks;
- Create enterprise-wide channels of communication about vendor usage, including plans to communicate with internal and external stakeholders following any incident; and
- Schedule a time to revisit the BCP to ensure that new vendors and threats are addressed.

Similarly, managing vendors needs to be an ongoing process, beginning with the contract and continuing for the length of the relationship. Some best practices for vendor management are to:

- Thoroughly vet vendors, conducting risk assessments and analyzing their cybersecurity capabilities (particularly with AI vendors, where the rush to market has left some vendors lacking in appropriate privacy and security measures);
- Create specific cybersecurity requirements in contracts, including NIST compliance and audit rights. Outlining security standards adds a greater chance for recovery in the event of a breach while also increasing the likelihood that the vendor has adequate safeguards;
- Assign risk and responsibility during a breach, including the response plan. Ensure that vendors have response plans that will minimize the impact on your organization;
- Keep an updated list of vendors and create a review-and-audit schedule. Identify high-leverage vendors and schedule times to review and audit their security systems and their impact on your business; and
- Create insurance obligations for vendors – particularly cybersecurity insurance – rather than relying on only your own coverage. Consider that many policies differentiate between the direct impact of a cyber incident and the resulting business interruption; carefully review policies and vendor contracts to ensure you have protections on both fronts.

Mitigating the operational risk from vendor relationships is a critical way to keep your business flexible and online when an incident inevitably occurs. If your organization needs assistance creating a vendor due diligence plan, drafting or reviewing contracts to ensure favorable protections, or undergoing business continuity planning, please contact the authors, Dan S. Parks, Layna Cook Rush, CIPP/US, CIPP/C, or a member of Baker Donelson's Data Protection, Privacy, and Cybersecurity team.