HORNE CYBER

Third-Party Risk—Why it Matters and Why it Isn't Going Away

Every organization faces risks, threats, and weaknesses because of their relationships with their vendors, whether financial or professional services, software vendors, janitorial, or building security services. The more you rely on your vendors to do business, the more access they have to your organization and your data, the greater the risk they present to you.

Yet, even as third-party ecosystems engulf the extended enterprise, organizations underrate and overlook the risks. By its own admission, Mercedes-Benz left customer data open to the world through a cloud vendor error three years before an independent security researcher reported it.

It's time to change your assessment and oversight of third-party risk. An increase in outsourced services is a hard trend that strengthens as more third-party services become available without geographic or time restrictions. Organizations increasingly outsource their critical processes, functions, and software development and have always outsourced raw materials to make products. With more vendors comes more risk.

According to Gartner, in 2019, 71 percent of organizations reported that their third-party network contains more third parties than it did three years ago; they said their third-party network would grow larger in the next three years (through 2022). Third-party risk will take up increasing real estate in your risk management program. You need to get ahead of it. You can start by understanding the vendor risks that every organization faces and accessing guidance on managing the risks.

HORNE CYBER

Operational & Financial Risks

Third-Party Risk Beyond IT

Risks to Operations

You count on your vendors' goods and services to run your business. If their services degrade or become unavailable, your operations could suffer.

Natural disasters and historical events can damage a vendor's ability to provide critical services. The pandemic infected employees and closed businesses across industries, picking apart the supply chains that kept organizations running.

Seventy percent of supply chain decision-makers said COVID-19 created the biggest supply chain impact, according to Jabil's Special Report, Supply Chain Resilience in a Post-Pandemic World.

Technical risks strike operations. If your software provider suffers a breach, and you rely on that vendor, you are immediately vulnerable and could go offline. You may not have the ability to perform essential functions if a vendor holds your data, and it becomes unavailable.

Ransomware attacks can encrypt your data at the vendor, making it inaccessible, or worse, your data could disappear indefinitely if the attack encrypts your vendor's backups. Ransomware attacks become unrecoverable when cybercriminals don't provide working decryption keys to unlock your data, even if your vendor pays the ransom.

Reputational risks transfer from third parties and become your operational concerns. If you're looking for a delivery service, you want to use a household name such as UPS or FedEx. If you use an unreliable service, it could become a dark spot on your reputation, creating operational challenges.

Good reputations evoke value and trust, and organizations get quality hires and increased revenues because of it, according to Reputation and its Risks, The Harvard Business Review. Your vendor is a direct extension of your reputation.

Financial Stability

Financial instability could affect your vendor's production or force them to close their doors. You need to know the state of your vendor's financials, including credit or fraud risks. Similar to the reputation risk, a vendor's financial stability will reflect on you, too.

HORNE CYBER

Your Extended Network

Cyber Risks & Third-Parties

Third-party vendors add cybersecurity risks. You give your vendors access to your networks, systems, and data for systems integrations and service performance. But criminal hackers count on your third-party's vulnerabilities so they can steal your credentials. Your vendor's access can quickly become the hacker's unauthorized backdoor into your systems. Then they can steal, alter, or destroy your intellectual property and customer databases when they take advantage of your vendor's vulnerability.

Don't think it can't happen to you. "Fifty-one percent of organizations experienced a breach caused by a third-party," according to a recent Ponemon report sponsored by SecureLink. It's not only your data that's at stake. Third-party breaches create reputational risks. Though cybercriminals use your third-party vendor to compromise your organization, your customers hold you accountable for the loss or exposure of their data.

Think of the companies that have had damaged reputations due to a third-party vulnerability. Target is the most widely known example. Criminal hackers breached the retail giant as a result of a vulnerability in its HVAC system. No one remembers the name of the HVAC vendor; they associate Target with the breach.

HORNE CYBER

Managing Third-Party Risks

You can address third-party risk by establishing a Third-Party Risk Management (TPRM) program. A TPRM program enables you to identify, measure, and monitor third-party risks. As you identify risks, you can ensure that your vendors use proper controls to mitigate the risks and apply a uniform risk rating system across your vendors as part of TPRM. You can arrive at consistent vendor risk scores, establishing low, medium, or high-risk vendors. Risk scores enable you to dial in vendor scrutiny. Because you rank and review your vendors similarly, you gain transparency into vendor risk across the organization.

A large part of managing third-party risks is performing due diligence before contracting with a vendor. Due diligence should include reviews of vendor reputation information, financials and SOC reports, and contractual obligations before committing to the relationship. SOC reports provide transparency into the vendor's security processes, financial stability, complementary controls, and Service Level Agreements (SLAs).

Vendors should adhere to SLAs or enact solutions in the agreement to restore services. Once you have established the SLA, it is critical to monitor it through the monthly reports the vendor agreed to provide to you.

Periodic vendor reviews should cover regulatory compliance based on the applicable industry. Confirm vendor compliance with Sorbanes-Oxley (SOX) and the Payment Card Industry (PCI-DSS) requirements when your vendor needs it. Vendors that fall under PCI-DSS must certify that they comply with it. During the initial review, assess the vendor's risk (high, medium, low) using your risk rating system and structure vendor contracts to align with your needs.

Repeat the review annually or more often, depending on the vendor's risk level. If the vendor's risk level has increased, you can decide whether and how you can continue using this vendor. You can use succession planning to have another vendor waiting should you need to replace them.

> **"Not taking risks one doesn't understand is often the best form of risk management," says Raghuram G. Rajan, Author, Fault Lines: How Hidden Fractures Still Threaten the World Economy.**

HORNE CYBER

Vendors responsible for your most precious information often escape risk management scrutiny. A data classification exercise will identify vendors holding sensitive data and allow you to incorporate them into the vendor management process and risk rating as appropriate.

Partner with your vendors in Business Continuity (BC)/Disaster Recovery (DR) Planning and plan execution. Play your role in assisting their recovery and enabling your own. Your vendor should share their plan with you and test it periodically alongside you. To plan for your own responsibility, be sure to document the timing and channels they will use to notify you of an incident.

Know what data your vendors back up and the kinds of backups they use. According to NIST Tips and Tactics for Dealing With Ransomware, it's essential to secure backups of your important data and make sure that you keep backups isolated so Ransomware can't spread to them. Because of this, you will want to confirm that your third-party isolates backups from production data.

Make sure that your third party's BC/DR plan establishes when you should disconnect from their services to avoid infection, such as with malware attacks, including Ransomware. The BC/DR plan should reveal the vendor's Recovery Point Objects (RPOs), so you know how much of your data they lost. The plan should discuss the vendor's Recovery Time Objectives (RTOs), so you understand how long it will take to restore your data. Plan your next move based on the BC/DR plan, so you can take action while the vendor is restoring your information. You may need to include in your plan how you will continue to operate without the data or services until they return.

Cyberattacks often occur as a result of inappropriate access, so pay special attention to unauthorized access. Apprise yourself of risks in the vendor environment that could permit people to perform privileged functions who have no need to do it. Insist on SOC certifications and review the reports to ensure that the vendor's processes and procedures related to access are secure. If you hire a vendor, you inherit their risks and potential for breaches.

"Risk comes with the territory when you are breaking new ground. Learn how to evaluate and mitigate these risks rather than take away people's power and autonomy," says Leena Patel, Author, Raise Your Innovation IQ: 21 Ways to Think Differently During Times of Change.

HORNE CYBER

Manage user access from the vendor to your applications, systems, and databases. Implement the principles of Least Privilege and Zero Trust. Least Privilege ensures that no vendor gets more access than they need to do their work. Zero Trust assumes you can't trust any user, entity, or machine. Instead, you must verify identities and the need for access and monitor user behavior for malicious activity.

Use Multifactor Authentication (MFA), so credential theft alone won't let cybercriminals inside your systems. People are your weakest link, so it's critical that you and your third parties immerse staff at all levels in security awareness training that applies to the risks you face.

One of the best ways you can be sure your third-party is checking for vulnerabilities and resolving any issues is to insist that they engage a penetration tester to find vulnerabilities at least annually. Be sure they are taking intentional steps to remediate the penetration test results in order to keep data secure. In addition to security tests and DR/BCP tests, third-parties should also test their incident response plan, and you need to know your role should a cyber incident occur.

Still Worth the Risk

These are many of the ways you can begin to mitigate the inherent third-party risks. However, Third-Party Risk Management offers no permanent solutions. It's a journey you can map proactively and steer decisively with ample visibility and plenty of recourse for unwieldy risk events. Practical solutions are as real as the risks, and you can find them.

Know more about third-party risk and what you can do **now.**
For questions, concerns, or a guiding hand, reach us at **sales@hornecyber.com.**

HORNE CYBER

Source List

1. Ponemon report. https://www.globenewswire.com/en/news-release/2021/05/04/2222054/0/en/51-of-Organizations-Have-Experienced-a-Data-Breach-Caused-by-a-Third-party-New-Report-Finds.html
2. Jabil. https://www.jabil.com/blog/covid-19-supply-chain-impact.html
3. NIST. https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware
4. Fault lines. https://www.amazon.com/dp/B00990IYBO/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1. See also https://www.goodreads.com/quotes/tag/risk-management.
5. Innovation IQ. https://www.amazon.com/Raise-Your-Innovation-IQ-Differently-ebook/dp/B07S8N517W. See also https://www.goodreads.com/quotes/tag/risk-management.
6. Mercedes-Benz. https://media.mbusa.com/releases/release-ee5a810c1007117e79e1c871352a4afa-mercedes-benz-usa-announces-initial-findings-of-data-investigation-affecting-customers-and-interested-buyers
7. Harvard. https://hbr.org/2007/02/reputation-and-its-risks.
8. Gartner. https://www.gartner.com/smarterwithgartner/a-better-way-to-manage-third-party-risk/