WHY YOUR THIRD-PARTY RISK MANAGEMENT STRATEGY **SHOULD ADDRESS CYBER RISK**

ARCHER™

INSIDE OUTSOURCING

Today's ongoing COVID-19 landscape, coupled with the War in Ukraine, has put into motion major business disruptions caused by cyberattacks, including cyberattacks targeting vendors that have a downstream effect. While companies turn to third-party vendors to assist with an increasing number of tasks, they are also relying more heavily on solutions in the cloud.

Outsourcing can save considerable money and boost efficiency. However, this strategy comes with its own set of potential security risks that should be examined and addressed before problems arise. Breaches can't be taken lightly, including those from external vendors that have the potential to adversely impact your business in numerous ways - take a toll on your bottom line, result in downtime, tarnish your reputation, affect compliance, and create fines, among other possible consequences.

ARCHER

FACTS AND FIGURES

Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.[1]

Gartner predicts that by 2025, 60% of organizations will use cybersecurity risk as a significant determinant in conducting third-party transactions and business engagements.[2]

Ponemon reports that 59% of data breaches are due to third parties.[3]

84% of organizations host critical or sensitive assets with external parties.[4]

[1] gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

[2] gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity--predictio

[3] Ponemon Institute, “Data Risk in the Third Party Ecosystem”

[4] riskrecon.com/internet-risk-surface-report

ARCHER

VULNERABILITIES

Enterprises have developed strategic dependencies with some third parties, leaving them vulnerable to sophisticated hackers who can gain access to a third-party's vendors, customers, and other partners. Therefore, employees, business partners, contractors, and IT service providers - everyone associated with your company's operations – must understand the importance of security when choosing to work with a third-party vendor and take it seriously. There are no shortcuts. Consider addressing cyber risk and vulnerability issues and practices in your contracts, so that your vendors understand what is expected of them. When it comes to cyber risk management, surprises are not welcome.

It is critical to understand how your third parties can leave you vulnerable because there are data breaches resulting from software libraries developed by third parties. An example of this is Log4J, which is a software logging library developed by Apache that organizations embed into their software instead of writing their own logging utility. Companies such as Apple, IBM, Oracle, Cisco, Google and Amazon use Log4J in their software. Software that use Log4J are VMWare, Minecraft, and Tableau server. Using this library leaves products and companies vulnerable and understanding your vendor's security policies is important to be able to help mitigate risk. Vendor assessments and continuously monitoring the security performance of an entire vendor catalog will enable you to be able to address issues.

ALL ABOARD

In today's digital and dynamic marketplace, companies no longer operate independently. Securing an organized, comprehensive, and ongoing Third-Party Security Risk Management (TPSRM) strategy - including on and off-boarding of third-party vendors - has become a must. With the cyber environment forever evolving, leadership must devise solid game plans to continuously monitor the security posture of all strategic vendors. There's no time to sit back and relax.

Being able to trust everyone in your business circle - and being confident that vendors have done their due diligence in implementing their own cyber risk and security measures - is now a necessity. That's why it's essential to maintain close relationships with everyone associated with your business. Make sure that members of your team are on the same page when security-related issues arise, so that these items can be promptly addressed and resolved. Developing powerful cyber risk management strategies allows you to leverage essential tools to circumvent potential problems. Such solutions can make significant contributions to the financial health and overall well-being of your company.

ARCHER

ON THE RIGHT TRACK

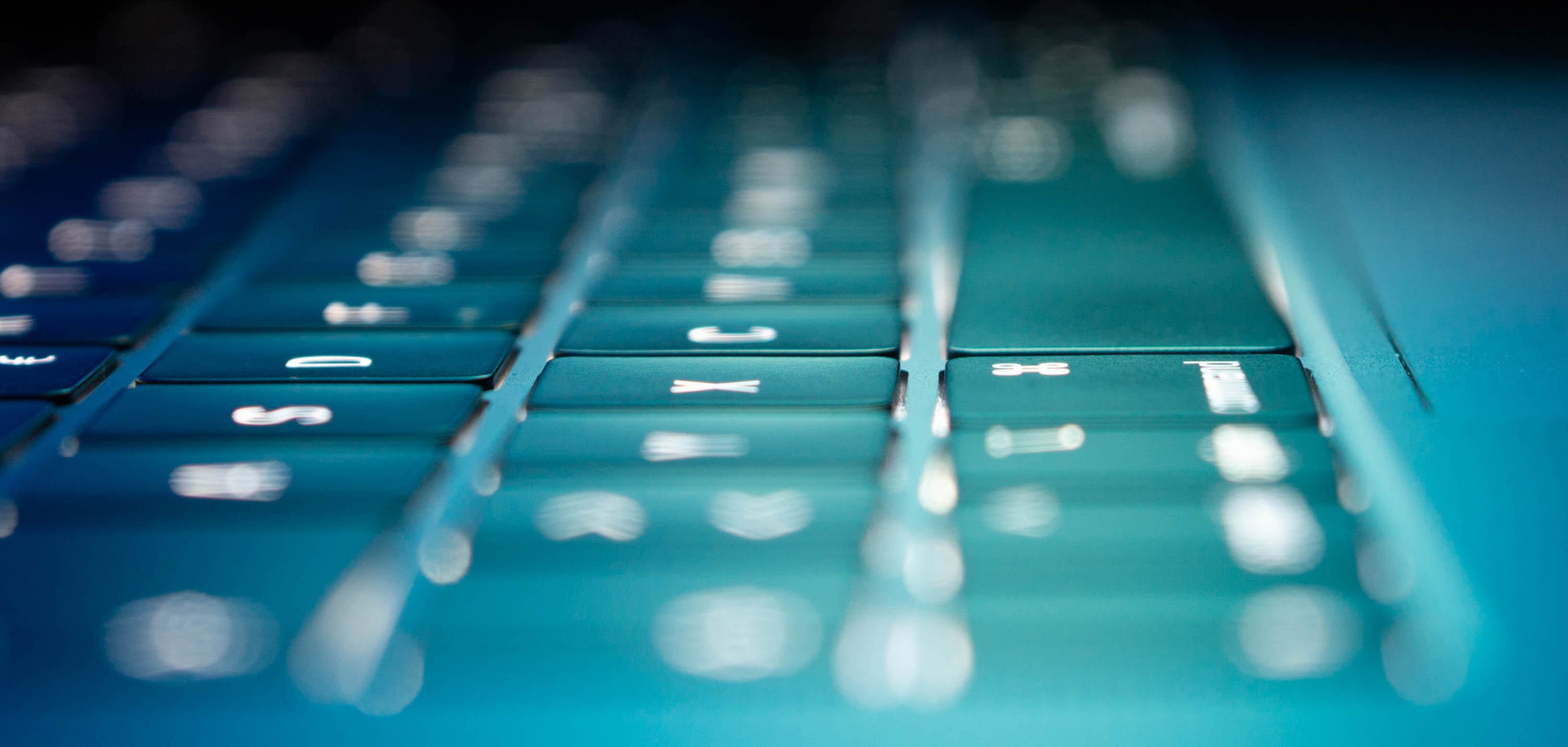
It's important to keep track of each one of your vendors and understand their cyber risk and security practices and policies. For those that are strategic to your business objectives or have access to sensitive data, extra diligence is mandatory. What precautions are these companies taking to keep your data safe and sound - and in the right hands?

Doing your due diligence to investigate the cyber risk practices of your third party vendors (and their vendors) is well worth the time, money, and effort. With the cloud here to stay, it has become increasingly more important to be proactive about protecting your company.

ARCHER

MAKING HEADLINES

Cyber risk is far-reaching and continues to threaten companies of all sizes in all industries and parts of the world. We witnessed this in 2020 with the attack on SolarWinds[1]. At the end of 2020, hackers targeted this prominent Tulsa, Oklahoma-based software company by inserting malicious code into its Orion IT monitoring and management software designed for global enterprises and government agencies. Thousands of organizations and government agencies were adversely impacted by this breach.



[1] Attack on SolarWinds - https://www.cisecurity.org/solarwinds

OPT FOR EMPOWERMENT

Companies must come from a place of empowerment - and not fear - by anticipating and examining breaches as if these breaches were happening right here and right now. It's wise to test out responses in "real time," so you're not caught off guard without a tangible and sound plan of action. Consider the risk level for each vendor, including how much interaction and exposure each vendor has to your data and other company resources.

SIX ESSENTIAL QUESTIONS

Here are six important questions to ask your third-party vendors from the get-go regarding their cyber risk management practices. Creating this dialogue sooner rather than later helps to alleviate serious and costly consequences. It also minimizes the risk of miscommunication going into these important business relationships and helps everyone involved realize the best possible outcomes. Asking the right questions and putting the appropriate practices into place early on is likely to result in a win-win for everyone involved.

1 Has the third-party developed a documented comprehensive cybersecurity risk management program that addresses and manages their own supplier ecosystem - including their partners and other providers. If so, please provide specific details.

2 Are third-party employees well educated on security awareness and kept up to date on phishing schemes and other security related concerns? If so, please provide specific details.

3 Explain the process and details regarding the plan your third-party vendor has in place to notify *your* company in cases of breaches or other security-related incidents?

4 How is the third-party vendor alerted in cases of potential unauthorized access to *their* own data?

5 Does your third-party vendor continuously monitor cybersecurity performance? If so, what is the process?

6 How well do your third-party vendors' Business Continuity (BCM) plans support your own operational resilience? Please provide specific details.

POWERFUL SOLUTIONS THAT GO THE DISTANCE

- **ARCHER THIRD PARTY GOVERNANCE** presents an accurate and complete picture of third-party risk and provides capabilities to manage and monitor your third party relationships and engagements' performance. It allows you to capture prospective relationships, engage affected stakeholders, assess contract risk, financial wherewithal, and inherent and residual risks across multiple risk categories, enforce risk-based selection of third parties and establish risk and performance metrics. With Archer Third Party Governance, you can automate and streamline oversight of your third-party relationships.

- **ARCHER THIRD PARTY SECURITY RISK MONITORING** enables you to assess third-party security risks quickly and more accurately with continuous, automated visibility into your vendors' IT landscape. Archer Third Party Security Risk Monitoring delivers actionable, objective insights about third-party security issues that pose the greatest risk to your business.

- **ARCHER ENGAGE FOR VENDORS** facilitates collaboration between business stakeholders, risk managers and external vendors throughout the governance lifecycle. An external and intuitive interface securely allows third-parties to efficiently complete assessments, questionnaires, upload documentation, respond to issues, and attest to performance enabling you to effectively manage third party risk.

ARCHER

ABOUT ARCHER

Archer is a leader in providing integrated risk management solutions that enable customers to improve strategic decision making and operational resiliency. As true pioneers in GRC software, Archer remains solely dedicated to helping customers understand risk holistically by engaging stakeholders, leveraging a modern platform that spans key domains of risk and supports analysis driven by both business and IT impacts. The Archer customer base represents one of the largest pure risk management communities globally, with over 1,500 deployments including more than 90 of the Fortune 100.

Visit ARCHER**IRM**.COM

ARCHER