To improve business resilience, strengthen your third-party partnerships

Jill M. Czerwinski, CIPP, CISA, CISSP
2/9/2021

When the next disruption occurs, can you count on your key vendors and suppliers? Follow these steps for better third-party resilience planning.

The global economic disruptions of 2020 revealed the myriad ways that businesses depend on third-party vendors and suppliers – and on what happens when they fail to

deliver. In some cases, supply chain interruptions brought companies' production to a standstill. In others, customer service call centers temporarily shut down as their vendors transitioned to remote work.

But some companies fared better with their vendor relationships. Their business continuity planning efforts considered not only their own ability to weather disruptions, but also the resilience of their third-party ecosystem of vendors and suppliers. They had effective ways of communicating both with their third parties and with their customers, and as a result, they improved their reputation and brand.

Such proactivity is a major takeaway for business resilience in 2021. Organizations also need to look beyond their walls and invest in strengthening third-party relationships. They should analyze whether the business continuity plans of their third parties match the detail and scope of their own.

Third-party successes and challenges: What COVID-19 has taught us

Businesses across major industries experienced similar COVID-19 disruptions among their vendors and suppliers, including:

Staffing shortages and slower responses. Reliance on third-party global service centers created challenges since many of these businesses were not prepared for the rapid transition to remote work. Remote work technology was often partially implemented, and personnel struggled to be fully productive working from home.

Lack of redundancy and diversity. Some manufacturers lacked adequate supply chain visibility and diversity. During the pandemic, they struggled to meet customer demand when their usual suppliers couldn't deliver raw materials and they hadn't previously set up alternative supplier relationships.

Cybersecurity risks. Some third parties exposed their client companies to new risks by failing to invest in cybersecurity measures. In their rush to set up remote working environments, they overlooked endpoint protections, making their clients' data vulnerable to phishing, patching problems, and other data breach culprits.

Some industries, like banking, were more prepared when managing vendors and suppliers. Many banks already had developed guidance for a pandemic response, both internally and among their vendor populations. They anticipated the need to switch

quickly from one vendor to another, and they made sure that critical vendors developed and maintained their own resilience plans.

Best practices to strengthen third-party resilience

To manage risk, businesses must address all phases of the third-party relationship management life cycle starting with an assessment of their vendors' risks and resilience. This assessment includes queries in written questionnaires such as:

- Does your organization maintain a business continuity plan?
- Does your business continuity program cover all in-scope systems, people, and facilities?
- Does your organization maintain a disaster recovery plan, and do you test your plan?
- Have you set realistic recovery objectives and considered redundancy in your plan?
- Do you have a documented incident management and response program?
- Does your incident management plan focus on effective communication, both from and to affected parties?

After reviewing a third party's plan and related documentation, a company can assess risks and gaps within the third party and whether its capabilities match the company's needed requirements. For example, a human resource department might require that a payroll vendor have its systems and data back online within 24 hours of an outage. This capability would then be formally reflected in a signed contract.

Finally, companies must establish ongoing engagements with their third parties, which might include periodic reevaluations and on-site inspections. Additionally, establishing a regular dialogue would build stronger and more trusted third-party relationships. Organizations should schedule time to get to know their vendor organizations and the people who run them in order to learn how their normal processes work and how recovery measures will take effect when a disruption occurs.

Navigating the phases of a third-party vendor relationship

There are five common phases to account for when working with a vendor. If after a periodic reevaluation you decide to stop working with a vendor, it's time to exit and terminate the relationship.

Proactive planning

Organizations that take proactive steps can help mitigate disruptions. Three suggestions for better third-party resilience planning include:

1. **Tracking issues to closure.** Too often an organization will identify a risk or process improvement for a vendor or supplier but then fail to confirm that the issue has been resolved. That failure to follow up sends a message to vendors that the issue isn't important enough, which makes them less likely to address it.
2. **Aligning organizational needs with third-party plans.** It's not enough for a vendor to have a business continuity plan. The plan needs to explicitly match the needs of an organization, including its recovery time objective (the duration of time needed to restore a service) and its recovery point objective (the maximum interval of time that can elapse between data backups).
3. **Outsourcing planning to a resilience professional.** Many organizations lack the in-house expertise necessary to evaluate vendors and supplier risks. A skilled consultant can perform assessments, align needs and capabilities to be reflected in contracts, and conduct reevaluations and inspections.

Business resilience begins with people

Organizational resilience depends more on people and relationships than on any single technology. The most resilient companies have established a **culture of empowerment** and preparation, in which trusted employees – as well as third-party vendors and suppliers – can be more agile and responsive.

The events of 2020 made many businesses better equipped to handle the next disruption or disaster. Thanks to remote work capabilities and stronger partner ecosystems, organizations can be more prepared. Their investments in resilience planning will pay dividends when, not if, the unexpected happens.

Contact us

Jill M. Czerwinski

Principal, Third-Party Risk Leader

+1 630 575 4317

Profile