KPMG

Voice of the CIO

A recurring conversation with CIOs on IT-related issues

October 2024

CIOs see their role expanded by third parties and adverse events

In our conversations with CIOs, we're sensing a shift in perspectives. Whether it was the impact from COVID-19 or systems going offline due to the global IT outage, CIOs are now asking tough questions about how third parties are managed and IT's role in company operations. They're learning that third parties also have suppliers that extend outward, and attestations don't do much to lower risk. CIOs are also getting a crash course in supply chain risk management and business continuity. They're starting to question the single-source model for vendor relationships. It's better to spread the risk with multiple vendors providing the same product or service. Doing so, though, adds cost. CIOs appreciate the company's business continuity program but are finding out that their role is limited. Many are starting to have thoughtful C-suite conversations about the vitalness of digital in operations and how IT risk is an enterprise risk. In light bulb moments, it's about resiliency and protecting the company's reputation.

On the CIO agenda

Revisiting the global IT outage

Lessons learned

The supply chain perspective

CIOs adopt supply chain strategies

Adapting to business continuity

An enterprise risk, not just IT

Revisiting the global IT outage

Lessons learned

It's been over two months since the global IT outage, but CIOs are still learning lessons from it. Even companies that weren't directly impacted by the outage felt the effects through their third parties.

"It's fundamental that we understand our critical data assets, applications, and what drives the company's revenue," said Marcus Murph, KPMG principal, CIO Advisory. "Companies should have backup recovery and resiliency plans for these crown jewels."

For CIOs, the global IT outage was an eye-opener that caused many of them to dig deeper into how they manage third-party risk. There is also a realization of the depth and complexity of third parties.

"We rely on checklists and attestations to verify what's happening with third parties, but it's more like an honor system," said a CIO of a major bank.

Another concern is the reliance beyond third parties. Outsourcing extends outwards, so a company's third parties also include fourth parties, fifth parties, and sixth parties. No company has controls and protocols that go that deep. It also varies from industry to industry. Regulated fields such as financial services have more mandates around the use of suppliers and their suppliers.

CIOs are also reviewing contracts for requirements around notifications and transparency. If a third party violates their contract, the CIO of a global automaker wonders about taking legal action. "If it's a technology outage that disrupts business, could we sue them? Are we prepared to weather the storm for three, five, seven days, if not a month, and what would it do to our business?"

It's a board-level issue around topics such as risk tolerance, business continuity, and scenario planning with discussions around blast radius and if one facility of ten needs to be shut down, what is the business case for the decision?

There are no easy answers, just more questions that have emerged after the global IT outage. One CIO consensus is a third party hit by an outage or a cyber incident may make a better partner versus a third party that has never been tested. In essence, the third party impacted has learned and made changes.

> "It's both business and technical resiliency that matter."
>
> Marcus Murph, KPMG CIO Advisory Leader

The supply chain perspective

CIOs adopt supply chain strategies

The global IT outage also changed CIOs' view of their world. IT and digital are now part of a connected ecosystem that can be disrupted by an inadvertent logic error. In essence, CIOs are thinking more holistically about their supply or value chains, and it's causing a reshuffling in how CIOs think about risk.

Business leaders are accustomed to contracting with a single supplier offering the best deal. CIOs are now seeing the inherent risk with single sourcing and how a single event can disrupt the supply chain. They're also discovering that many of their suppliers are technology based and subject to the same kind of disruptions common within their own companies. One work-around is to create redundancy.

"We're going to need multiple partners on a capability, and we may not go with the best deal," said a healthcare technology CIO. "Ultimately, we'll split volume across multiple vendors."

CIOs with a greater appreciation for supply chain risk stand ready to switch suppliers because of greater reliability or a lower risk of something going awry. It's all about minimizing risk. CIOs also have something of value to offer C-suites in their discussions. It's the unique tech perspective that only CIOs possess.

Other CIOs are borrowing from the supply chain risk management playbook with tactics such as improved onboarding procedures, more detailed assessments, better controls, ongoing monitoring, and data sharing. With advanced knowledge, a CIO can switch to a different supplier based on its IT services.

One enterprising CIO is using a red, blue, purple teams approach common with cybersecurity. Why?

"It's going after every possible break in the link that will disrupt our business in small ways and big ways," said the CIO.

There is even frank discussion among CIOs about the risk of relying on major cloud providers that supply network services. They've experienced outages as well. But how practical is it to do business with multiple cloud providers given the current demand on resources?

For CIOs, it's about asking the right questions. In C-suite meetings, it's CIOs elevating the dialogue to make sure the business is resilient should disaster strike that impacts operations.

Adapting to business continuity

An enterprise risk, not just IT

CIOs are becoming more versed in business continuity. Whether it was thinking back to COVID-19 or the more recent global IT outage and the widespread impact from both, CIOs are seeing the value of a business continuity program that helps organizations recover from disasters and disruptions.

"Business continuity encompasses enterprise risk, not just a tech risk," said a healthcare technology CIO with a more expansive view of his duties.

There is just one challenge. In most cases, business continuity does not sit in the IT organization. For another CIO, he owns recovery from a tech outage but has no say in business continuity. Risk, compliance, or a business continuity manager typically runs the program.

CIOs have an excellent strategy for being influencers in the company's business continuity program. When systems and data go offline, the disruption impacts the company's bottom line.

The CIO of an auto manufacturer has his own approach to business continuity.

"I just want to contractually ensure we're protected as much as we can, passing risk along, but also knowing what leverage can be used against third parties."

Meanwhile, another CIO shared the concept of failure-based design. It kicks in when failures happen. The goal is to isolate the failure and then ensure the rest of production is operational.

"We are so digitally connected these days that one issue in one place can have a cascading effect across the organization," said the CIO for an energy company. "Every time a system is down, you're leaving money on the table."

When operations are disrupted for too long, it can lead to reputational risk. Companies that are concerned about reputational risk are always response ready.

"Concentrated on the business side, we're ready with our reputation risk message," said the CIO for a major bank that is required to have a very robust recovery business continuity plan.

How much can CIOs take on with business continuity given their current responsibilities? For a CIO with a financial services company, the issue is budget and feasibility. Their advice:

"Pick the risk areas you want to be more thoughtful about and prioritize those."

> "Every time a system is down, you're leaving money on the table."
>
> Energy company CIO

Takeaways

- Review and update third-party risk management processes
- Journey map the value chain and identify weak links
- Contribute IT perspective to the business continuity program

Additional insights

Make operational resilience your North Star

Be organizationally and operationally resilient when—and where—it matters

2024 KPMG US technology survey report: The digital dividend

Marcus Murph
CIO Advisory Leader
KPMG LLP
T: 214-840-2671
E: marcusmurph@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**