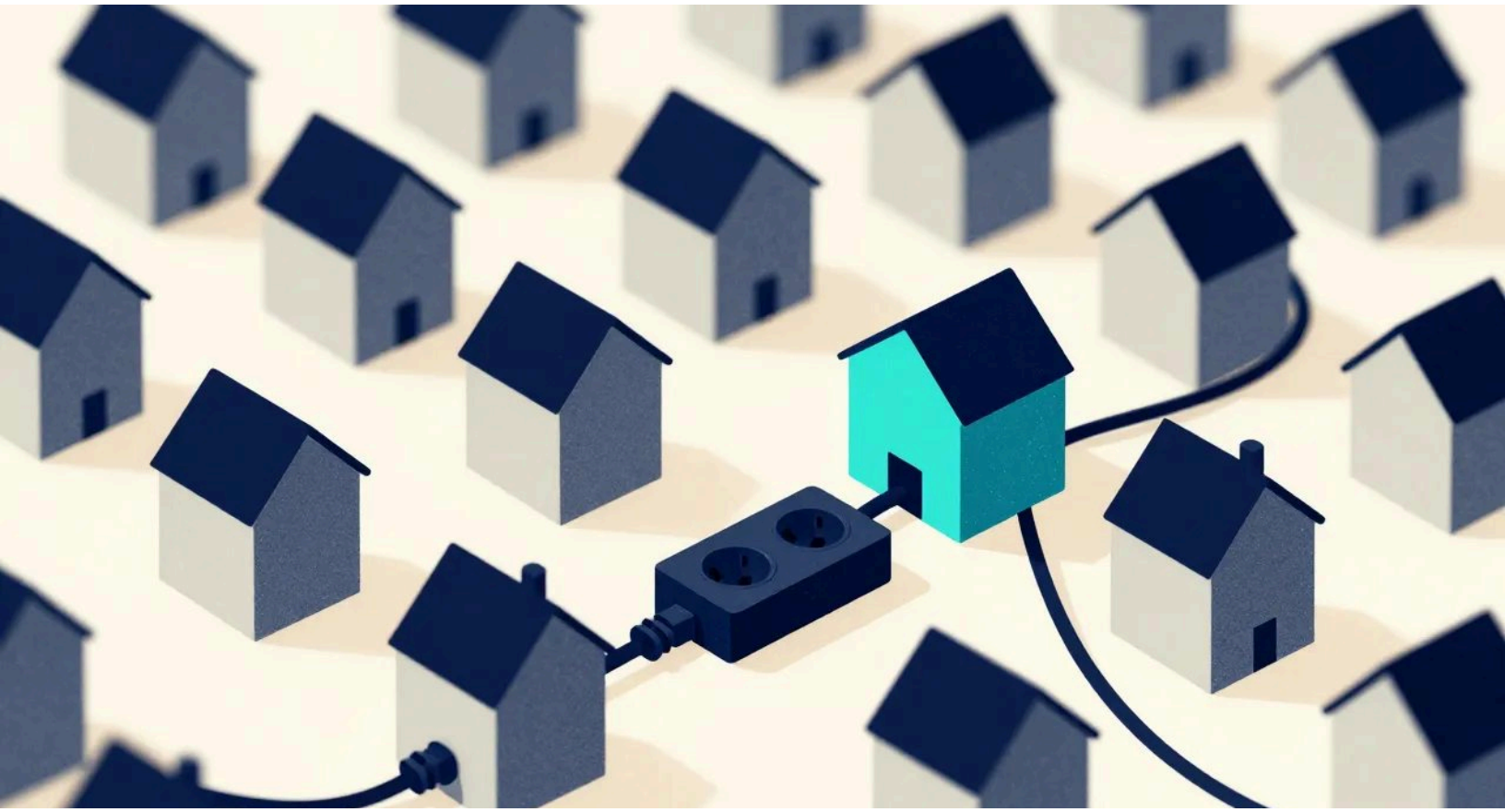


EXECUTIVE PAPER · DISASTER RECOVERY

Your Provider's Outage Is Your Outage

Cloud, software and security vendors now cause most publicly reported outages. Boards that treat vendor failure as someone else's problem are carrying a concentration risk they have never measured.

AUTHOR

Chris Watkins

SERVICE

Disaster Recovery

FOR

CEO, Board · 12 min read

AT A GLANCE

The problem. Third-party providers account for about two-thirds of publicly reported outages. A single faulty update or configuration change at one vendor can stop thousands of companies at once, and customers blame the company they buy from.

Why it persists. Vendor risk is run as procurement: questionnaires, certifications and service credits. Few companies know which of their critical services share the same cloud region, security agent or software platform, and few have tested what they would do without them.

The recommendation. Build a dependency map of critical services and the vendors beneath them, including the vendors' own providers. Rank each vendor by how many critical services it touches and how hard it is to replace. Then choose a response for each: accept, buffer, diversify or prepare to exit. Report the top concentrations to the board, as European and UK financial regulators now require of the firms they supervise.

The Decision in Front of You

Payments, customer service, identity, endpoint security, networking and hosting now sit with a handful of providers at most companies. When one of them fails, the company is down, and its customers, regulators and shareholders hold the company accountable.

The board decides whether that exposure is managed as a business risk with an owner, a measure and a plan, or left with procurement. One faulty security update in July 2024 cost the largest US companies an estimated $5.4 billion, and insurance was expected to cover a small fraction of it [5].

What's Happening

Third parties cause most public outages

Over nine years of tracking publicly reported outages, Uptime Institute found that third-party IT and data center providers, including cloud and internet companies, telecoms and colocation firms, accounted for about two-thirds of them [1]. Its 2026 analysis found fiber and cable problems were the leading cause of public IT outages in 2025, and telecom outages rose well above their 2020 to 2025 average [2]. Third-party outages are most often linked to software and configuration errors [2].

About four in five operators run their own risk assessments, but only 39% assess systemic third-party risk [2]. Only 18% of organizations surveyed insure against cloud provider outages [2].

Recent cases

CrowdStrike, July 2024. On July 19, 2024, CrowdStrike pushed a content configuration update to its Falcon sensor for Windows [4]. The update crashed the machines it reached. Microsoft estimated 8.5 million Windows devices were affected, under 1% of all Windows machines, and CISA confirmed the cause was the update and no attack [3]. The small share mattered less than where those machines sat, in airlines, health care and banking [5]. Parametrix, a cloud outage insurer, estimated direct losses of $5.4 billion for the US Fortune 500 excluding Microsoft. About a quarter of those companies were affected, including every airline in the group, and insurance was expected to cover only 10% to 20% of the loss [5].

Delta Air Lines canceled about 7,000 flights over five days, affecting 1.3 million customers, and put its cost at $500 million or more [6]. Delta and CrowdStrike then disputed responsibility in public [6]. The vendor's error became Delta's operating loss, and any recovery from the vendor would come later, through a dispute.

Cloudflare and its cloud provider, June 2025. On June 12, 2025, Cloudflare lost a set of its own services for about two and a half hours [7]. The cause sat one layer further down: part of the storage behind its Workers KV product ran on a third-party cloud provider that was having its own outage. About 90% of Workers KV requests failed, and Cloudflare Access failed every identity-based login during the event [7]. Companies that used Cloudflare Access for employee sign-in were relying on a cloud provider they had no contract with and had never assessed. Cloudflare committed to removing the dependency on any single provider for that storage [7].

CDK Global, June 2024. CDK supplies the dealer management software used by more than 15,000 car dealership locations in the US and Canada. After two cyber incidents, it shut its systems down on June 19, 2024, and many dealers went back to paper [8]. Anderson Economic Group estimated dealer losses above $600 million in the first two weeks, and projected $944 million if the outage ran into a third week [8]. One vendor serving thousands of dealers turned its outage into theirs.

Two 2025 cloud events reinforce the pattern. An AWS DNS fault in Northern Virginia disrupted most services in that region for up to 15 hours in October [9]. Nine days later, a configuration change at Microsoft's Azure Front Door caused about eight hours of disruption across Azure services, including Entra ID, Microsoft's identity platform [10].

SIDEBAR: FOURTH PARTIES

A fourth party is your vendor's vendor. The Cloudflare outage of June 2025 traced to a cloud provider most Cloudflare customers had no contract with [7]. Two vendors that look independent on a contract list can fail together because they sit on the same platform.

Regulators have moved first in finance

European and UK financial regulators now treat concentration on technology providers as a systemic risk.

The EU's Digital Operational Resilience Act, Regulation (EU) 2022/2554, requires financial firms to keep a register of every ICT services contract, distinguish the ones that support critical or important functions, and report it to supervisors [11]. For those critical contracts, firms need documented exit strategies that are tested and reviewed periodically, with identified alternatives and transition plans [11]. Before signing, they must assess whether the provider is easy to substitute and whether the contract adds to existing reliance on the same or closely connected providers [12]. On November 18, 2025, the European Supervisory Authorities designated 19 critical ICT third-party providers for direct oversight, using data from those registers [13][14]. Where a provider ignores remediation, supervisors can, as a last resort, require financial firms to suspend or terminate its services [14].

In the UK, HM Treasury designated Amazon Web Services, Google Cloud, Microsoft and Oracle as critical third parties, and the Bank of England, the PRA and the FCA began overseeing them on July 13, 2026 [15]. The regulators state that regulated firms remain responsible for their own due diligence, risk management and contingency planning [15].

The rules bind only financial firms, though the same reasoning fits any company whose revenue depends on a few providers.

Why the Usual Approach Fails

Vendor management in most companies is a procurement function that checks for a SOC 2 report and signs a contract with an availability target. None of that measures concentration.

Service credits are small. In the author's experience they are a percentage of the monthly fee for the affected service, which is tiny next to lost revenue. Even insurance closes little of the gap: in the CrowdStrike estimate, insured losses were 10% to 20% of the total [5].

Dependencies hide in layers. A company may hold separate contracts for identity, customer support, payments and hosting, and assume it has spread its risk. If three of those run on the same cloud region or behind the same edge network, one failure takes them all, as Cloudflare's customers learned [7].

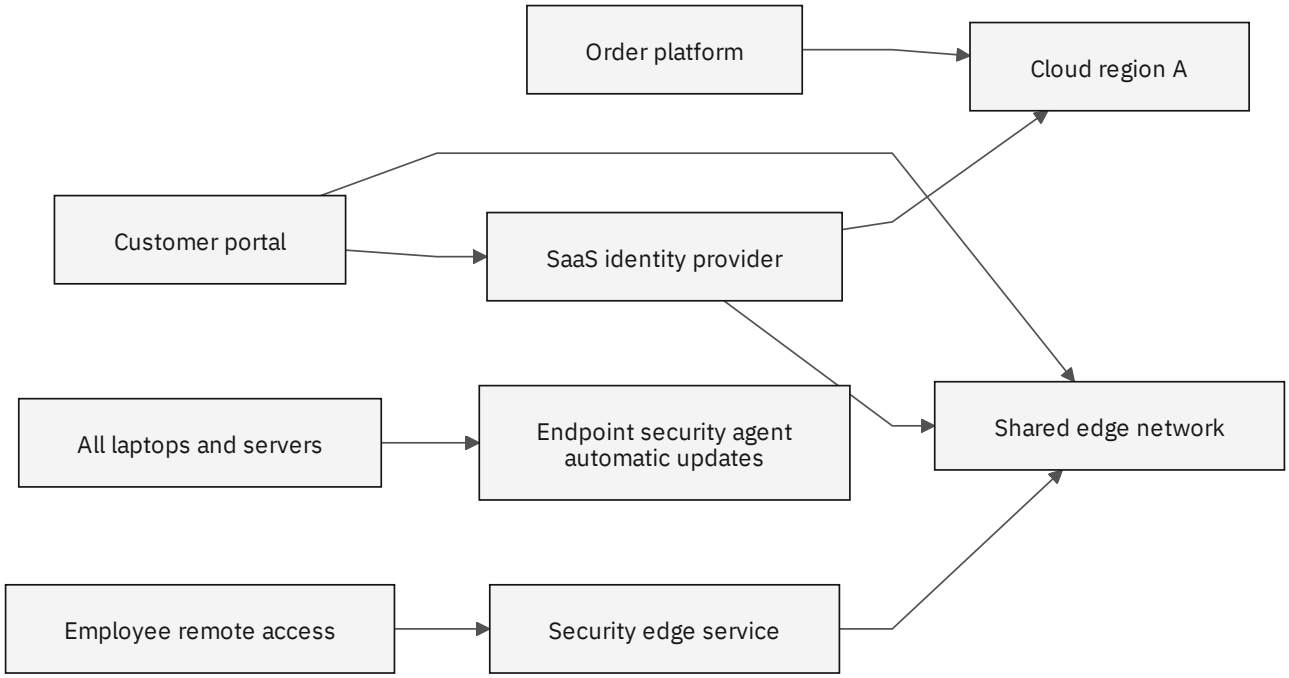
Shared failure feels safe, since customers seem to forgive an outage that hits half the internet. Delta's $500 million shows what a shared outage can still cost one company [6].

Exit plans exist only on paper. A plan to move off a critical vendor that has never been rehearsed gives no reliable estimate of how long the move would take. DORA requires exit plans for critical services to be sufficiently tested [11].

The Framework: Map, Rank, Respond

The approach has three steps and four possible responses per vendor.

Exhibit 1. A dependency map shows concentration that a contract list hides



Source: author's illustration of a hypothetical organization. Four critical services appear to use four vendors; tracing one layer down shows two shared dependencies and one agent installed everywhere.

Map. For each critical service, list every vendor it needs to run, then ask each of those vendors which cloud, network and software providers they depend on. Include software that runs on your own machines and updates itself, such as endpoint security agents, since CrowdStrike showed that an agent installed everywhere is a single point of failure [3][4].

Rank. Score each vendor on the number of critical services that stop if it fails and on the time needed to replace it or work around it. DORA's pre-contract test looks at the same two factors: substitutability and accumulated reliance on one provider [12].

Respond. Assign each vendor one of four responses, owned by a named executive.

Exhibit 2. Illustrative concentration register for a hypothetical company

Vendor	Critical services affected	Time to replace	Response
Primary cloud region	4 of 6	6 to 12 months	Buffer: second region for the order platform; tested failover
Endpoint security agent	All devices	3 to 6 months	Buffer: staged update rings; tested mass recovery of devices
SaaS identity provider	5 of 6	6 months	Buffer: break-glass accounts and cached access for operations staff
Dealer or industry platform	2 of 6	12 months or more	Exit plan: data export monthly; manual procedures rehearsed yearly
Edge network and DNS	3 of 6	1 to 3 months	Diversify: secondary DNS and a second edge provider for public sites
Payroll SaaS	0 of 6	3 months	Accept: monitor and communicate

Source: author's illustrative example. Vendor categories reflect the cases in this paper; counts and times are hypothetical.

Accept the risk where a vendor supports nothing critical, and say so in writing. **Buffer** where replacement is slow: add caching, manual fallbacks, staged updates and break-glass access so the business keeps working while the vendor recovers. **Diversify** where a second provider is cheap and the switch can be automated, as with DNS. **Prepare to exit** where a vendor is critical and hard to buffer: keep data exportable, contracts terminable and an alternative identified, as DORA asks of financial firms [11].

Costs, Risks, and Tradeoffs

Exhibit 3. Tradeoffs of managing provider concentration

Area	Cost or risk	Mitigation
Mapping effort	Tracing fourth parties takes staff time and vendor cooperation	Start with the top six critical services; require dependency disclosure at renewal
Second providers	Running two providers raises cost and adds integration work that can itself fail	Diversify only components with simple, standard interfaces such as DNS and edge delivery
Buffering	Manual fallbacks decay if they are never used	Rehearse each fallback at least once a year with the staff who would run it
Negotiating power	Large providers rarely accept custom terms	Focus negotiation on data export, incident notice and update controls instead of credits
Slower updates	Staged update rings delay security fixes	Keep the first ring small and fast; set a maximum delay for the last ring
When this is wrong	A small company with no in-house engineers and few critical services gains little from multi-provider designs	Choose mature providers, keep data exportable and buy insurance that covers provider outages

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	Name an executive owner for third-party resilience. List the six most critical services and every vendor each one needs.	CEO assigns; COO or CIO owns	Owner named; first vendor list for six services
First 90 days	Ask each critical vendor for its own hosting, network and software dependencies. Build the dependency map and concentration register. Score each vendor and assign a response.	CIO with procurement and security	Register complete; every vendor has a response and an owner
First 90 days	Put self-updating agents on staged rings where the vendor allows it. Create break-glass access that does not depend on the primary identity provider.	Security lead	Staged rings live; break-glass access tested
First 365 days	Rehearse a full outage of the top two concentrations, including manual operation and customer communication. Test one exit plan by exporting and restoring data in an alternative.	COO with CIO	Two rehearsals completed; one exit plan tested with recorded time to restore
First 365 days	Report the top five concentrations, their responses and test results to the board or its risk committee. Add dependency disclosure and data export rights to renewal terms.	CIO with general counsel	Board report delivered; renewal terms updated for critical vendors

Source: author's recommendation.

Questions to Ask Your Team

1. Which single vendor, if it failed tomorrow, would stop the most revenue?
2. Which of our critical vendors run on the same cloud region or edge network?
3. What software updates itself on every laptop and server, and can we stage those updates?
4. How would staff sign in to critical systems if our identity provider were down for a day?
5. For our most critical platform, how long would it take to move to an alternative, and have we ever tested the data export?
6. What would our service credits pay out against a 24-hour outage, compared with the revenue lost?
7. Does our insurance cover losses from a provider's outage?

Closing

Customers see your company failing to take an order, board a passenger or open a medical record, and the vendor behind it stays invisible to them. Map the vendors beneath your critical services, rank the concentrations, give each one an owner and a response, and test the responses before a provider's outage tests them for you.

Sources

[1] Uptime Institute. "Uptime Announces Annual Outage Analysis Report 2026." Press release via Business Wire. 2026. https://www.businesswire.com/news/home/20260513289344/en/Uptime-Announces-Annual-Outage-Analysis-Report-2026.

[2] Uptime Institute. "Annual Outage Analysis 2026." 2026. https://datacenter.uptimeinstitute.com/rs/711-RIA-145/images/2026.AnnualOutageAnalysis.pdf.

[3] Cybersecurity and Infrastructure Security Agency. "Widespread IT Outage Due to CrowdStrike Update." Alert. 2024. https://cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update.

[4] CrowdStrike. "Channel File 291 Incident: Root Cause Analysis is Available." 2024. https://crowdstrike.com/blog/channel-file-291-rca-available.

[5] Parametrix. "CrowdStrike to Cost Fortune 500 $5.4b; Insured Loss Range of $0.54b - $1.08b." 2024. https://www.parametrixinsurance.com/in-the-news/crowdstrike-to-cost-fortune-500-5-4-billion-insured-loss-range-of-540-million-to-1-08-billion.

[6] Insurance Journal. "Delta Rejects CrowdStrike Criticism, Sees $500 Million Hit From Cyber Outage." 2024. https://amp.insurancejournal.com/news/national/2024/08/09/787765.htm.

[7] Cloudflare. "Cloudflare service outage June 12, 2025." Post-mortem. 2025. https://blog.cloudflare.com/cloudflare-service-outage-june-12-2025/.

[8] Fox Business. "Car dealership losses from CDK software outage could soon reach $1 billion, study finds." Coverage of Anderson Economic Group estimate. 2024. https://www.foxbusiness.com/markets/car-dealership-losses-from-cdk-software-outage-could-reach-1-billion-study-finds.

[9] InfoQ. "AWS DynamoDB outage postmortem." Coverage of the AWS service disruption summary. 2025. https://www.infoq.com/news/2025/11/aws-dynamodb-outage-postmortem.

[10] ThousandEyes. "Microsoft Azure Front Door outage analysis, October 29, 2025." Citing Microsoft's preliminary post-incident review. 2025. https://www.thousandeyes.com/blog/microsoft-azure-front-door-outage-analysis-october-29-2025.

[11] European Union. "Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)." Article 28, General principles. OJ L 333, 27.12.2022. Via Springlex. https://www.springlex.eu/packages/dora/dora-regulation/article-28/.

[12] European Union. "Regulation (EU) 2022/2554 (DORA)." Article 29, Preliminary assessment of ICT concentration risk at entity level. OJ L 333, 27.12.2022. Via Springlex. https://www.springlex.eu/en/packages/dora/dora-regulation/article-29/.

[13] European Banking Authority. "European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act." Press release. 2025. https://www.eba.europa.eu/publications-and-media/press-releases/european-supervisory-authorities-designate-critical-ict-third-party-providers-under-digital%5C.

[14] Morgan Lewis. "DORA: EU regulators announce list of critical ICT third-party providers." 2025. https://www.morganlewis.com/blogs/sourcingatmorganlewis/2025/11/dora-eu-regulators-announce-list-of-critical-ict-third-party-providers.

[15] Financial Conduct Authority. "UK financial regulators to begin overseeing Critical Third Parties announced by Treasury." Statement. 2026. https://www.fca.org.uk/news/statements/uk-financial-regulators-overseeing-critical-third-parties-announced-treasury.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.