

The Risk You Can't See

How hidden dependencies create business exposure

You cannot always prevent the event. But you can often prevent the event from becoming a business crisis.

Recent disruption to the UK's air traffic control system provides a powerful reminder of something that businesses in every sector should be asking themselves:

How exposed are we to something we believe is unlikely to happen?

In September 2026, a technical failure within the UK's National Air Traffic Services (NATS) flight-processing system caused widespread disruption across UK aviation. The original technical problem was resolved, but the consequences continued well beyond the initial failure.

More than 2,000 flights were cancelled, disruption affected airports across the UK and hundreds of thousands of passengers, while airlines were left dealing with the knock-on effects of aircraft, crew and passenger displacement.

The UK Transport Secretary subsequently said that she did not believe the disruption was unavoidable and ordered further investigation into what happened and how the resilience of the system could be improved.

There is an important lesson here for every organisation.

It isn't simply about whether a system can fail.

It is about what happens to your business when it does.

Risk is not the same as exposure

Most organisations have risk registers.

They identify suppliers, systems, processes and events that could potentially cause disruption. They assign probability and impact scores. They put mitigation plans in place.

But there is often a fundamental gap between **knowing that a risk exists** and **understanding your exposure to it**.

Consider a critical technology supplier.

The organisation may know that:

- the supplier is strategically important;
- the system is business critical;

- an outage is possible;
- the supplier has business continuity arrangements;
- the contract contains service levels;
- the supplier has a disaster recovery plan.

On paper, the risk may therefore appear to be controlled.

But ask a different question:

What happens if the system becomes unavailable at 9am tomorrow and remains unavailable for 48 hours?

Suddenly the assessment becomes much more interesting.

Can the business continue?

Which processes stop?

How much revenue is at risk?

Which customers are affected?

Can employees work around the problem?

Is there another supplier?

How quickly could it be implemented?

Can data be extracted?

Does the contract actually provide practical exit rights?

Does anyone know how to execute the contingency plan?

And perhaps most importantly:

Has the organisation ever tested it?

That is the difference between identifying risk and understanding exposure.

The hidden dependency problem

Modern businesses are built on dependencies.

Some are obvious.

Others are buried several layers beneath the surface.

Your business may depend upon:

A supplier

↓

A technology platform

↓

A cloud infrastructure provider

↓

A third-party integration

↓

A subcontractor

↓

A critical data source

The organisation may have a direct contractual relationship with only one of these parties.

Yet a failure several layers down can still affect the business.

This is why supplier risk assessments that focus solely on the immediate supplier can provide a false sense of security.

The same applies to technology, outsourcing, logistics, finance, manufacturing and increasingly AI.

A dependency does not need to be owned by your organisation to become your problem.

The illusion of resilience

One of the most dangerous assumptions businesses can make is:

“We have a plan, therefore we are resilient.”

A contract is not resilience.

A disaster recovery plan is not resilience.

A second supplier is not necessarily resilience.

Insurance is not resilience.

A backup system is not necessarily resilience.

These things may all contribute to resilience.

But the real question is whether they would work **when you actually need them**.

For example, an organisation may have contractual termination rights allowing it to exit a supplier relationship.

But if the supplier holds critical data in a proprietary format, there is no alternative supplier available and migration would take twelve months, the contractual right to terminate may provide little practical protection.

Likewise, an organisation may have identified a second supplier.

But if that supplier has never been onboarded, has insufficient capacity and has never been tested, it may not represent a genuine alternative.

Resilience needs to be assessed against reality, not documentation.

From risk to exposure

At Heavy Salad, we believe it is useful to think about risk as a chain:

Dependency → Failure → Impact → Exposure → Consequence

The dependency is what the organisation relies upon.

The failure is the event that interrupts it.

The impact is what happens operationally.

The exposure is the extent to which the organisation is unable to absorb or mitigate that impact.

The consequence is the eventual business outcome.

This distinction matters.

Two organisations can have exactly the same dependency and exactly the same failure.

But their exposure can be completely different.

One may have:

- alternative suppliers;
- redundant technology;
- transferable data;
- tested contingency arrangements;
- sufficient internal capability;
- strong contractual protections;
- insurance;
- financial reserves;
- rehearsed recovery plans.

The other may have none of these.

Same risk. Very different exposure.

The five questions businesses should be asking

Before concluding that a critical risk is adequately controlled, organisations should be able to answer five basic questions.

1. What are we critically dependent upon?

- Not just direct suppliers.
- Look across technology, people, suppliers, subcontractors, infrastructure, data, processes and third parties.

2. What happens if it stops working?

- Don't describe the impact in generic terms such as "business disruption".
- Identify the specific operational, financial, customer, regulatory and reputational consequences.

3. How quickly can we recover?

- What is the realistic recovery time?
- Not the recovery time stated in a supplier presentation.
- The time your organisation could actually operate without the dependency.

4. What alternatives do we genuinely have?

- An alternative that exists only on paper isn't an alternative.
- Can it provide the required service?
- Does it have capacity?
- How quickly could it be activated?
- Has it been tested?

5. What evidence do we have?

- This is perhaps the most important question.

What evidence demonstrates that our mitigation would work?

If the answer is simply “the supplier has told us”, “we have a policy” or “we have a contract”, the organisation may have identified the risk without actually reducing its exposure.

Avoiding exposure rather than managing the aftermath

Traditional risk management often focuses on mitigation.

Heavy Salad takes a slightly different perspective.

We believe organisations should also ask:

Can we identify and reduce our exposure before the risk materialises?

That means looking beyond the risk register and examining the underlying dependencies.

It means challenging assumptions.

It means testing whether contractual protections are actually usable.

It means examining whether supplier alternatives are real.

It means understanding where data, technology and operational capability are concentrated.

It means identifying the points where a relatively small failure could create a disproportionately large business impact.

And it means doing this **before the incident happens**.

Because once the failure occurs, the organisation is no longer managing risk.

It is managing consequences.

The Heavy Salad approach

Our approach is simple:

IDENTIFY

Identify the dependencies, vulnerabilities and critical points of failure.

ASSESS

Assess the probability, impact and — crucially — the organisation's actual exposure.

CHALLENGE

Challenge assumptions, controls, contracts, supplier claims and contingency arrangements.

QUANTIFY

Translate potential disruption into business impact wherever possible.

ACT

Prioritise the actions that will materially reduce exposure.

This approach can be applied across procurement, supplier management, contracts, technology, operating models and business processes.

It is particularly valuable where an organisation has become dependent upon a supplier, technology platform or process without fully understanding what would happen if that dependency failed.

The question organisations should really be asking

The lesson from major failures is often framed as:

“How do we stop this happening again?”

That is an important question.

But it isn't the only question.

A more useful question may be:

“If this happens again, are we better prepared than we were last time?”

And there is an even more fundamental question:

“What other risks are sitting quietly in our business today that could create a similar level of exposure?”

You cannot predict every failure.

You cannot eliminate every risk.

And you cannot build a completely risk-free organisation.

But you can identify critical dependencies.

You can understand where exposure sits.

You can challenge whether existing controls would actually work.

And you can take action before a risk becomes a crisis.

Don't wait for the failure to identify the exposure

The most expensive time to discover a critical dependency is **after it has failed**.

The most expensive time to discover that your supplier exit provisions don't work is **when you need to exit**.

The most expensive time to discover that your contingency plan has never been tested is **when the primary system is unavailable**.

And the most expensive time to discover that your business is exposed is **when someone else discovers it first**.

Heavy Salad exists to help organisations identify those exposures before they become problems.

Because sometimes the biggest risk isn't the one you know about.

It's the one you haven't yet identified.

Heavy Salad

Identify the risk. Understand the exposure. Take action before it matters.

Our diagnostic assessments are designed to help organisations look beneath the surface, identifying vulnerabilities, dependencies and areas of potential exposure across procurement, suppliers, contracts, technology and business operations.

Don't wait for the failure to tell you where your exposure is.

www.heavysalad.co.uk