sphera

Too late to act in supply chains

HOW DELAYED DETECTION AND FRAGMENTED DECISIONS TURN SUPPLY CHAIN RISK INTO RECURRING REVENUE LOSS

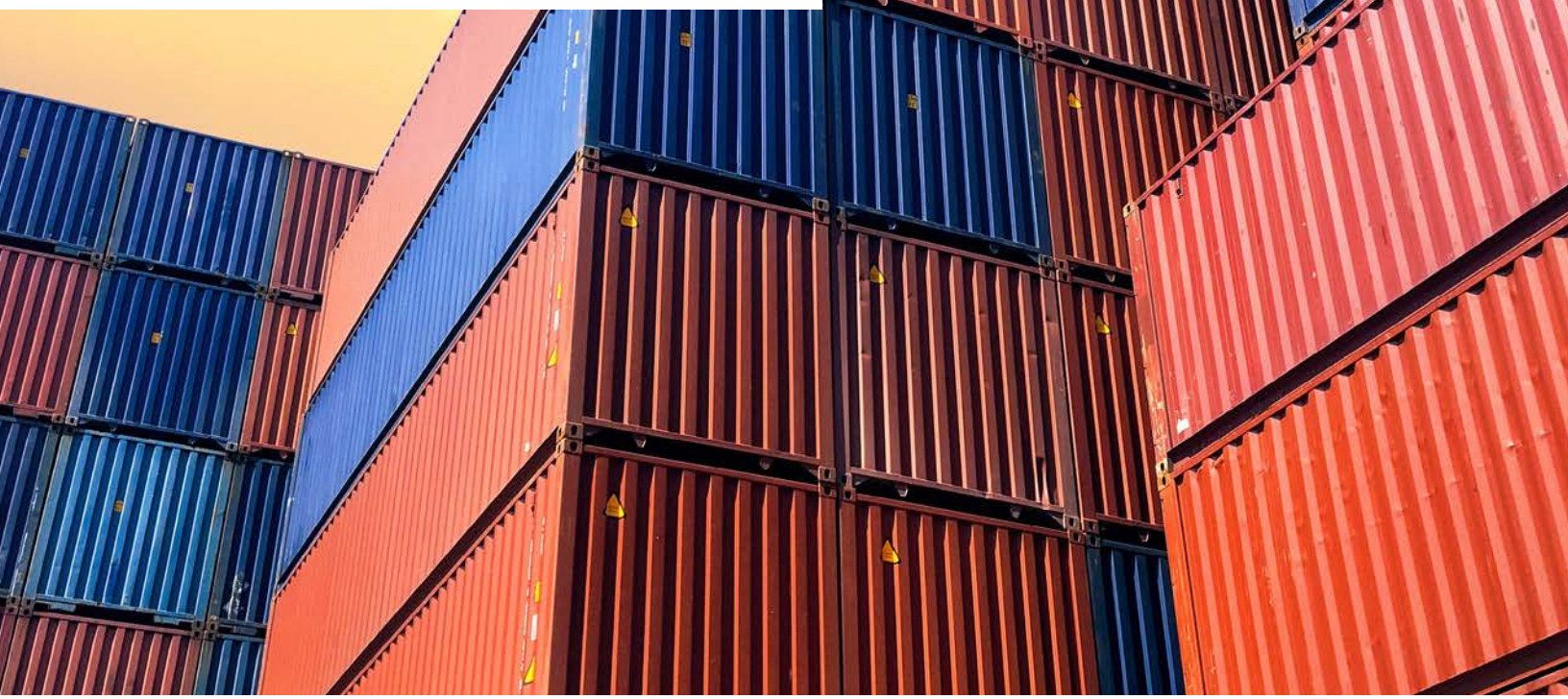
Contents

Supply chain risk is no longer a visibility problem, it is a timing problem.

Organizations today can identify disruption signals, but they are still too slow to translate those signals into decisions and action. As geopolitical instability, supplier fragility, and operational complexity increase, the ability to act early is becoming the primary determinant of financial and operational outcomes.

To understand how organizations are managing this shift, Sphera surveyed 200 CFOs and COOs across Manufacturing, Chemicals, Aerospace & Defense and CPG. The findings reveal a consistent pattern: visibility is improving, but detection is delayed, decision-making is slow, and execution is not systematized.

The result is a structural gap between knowing and acting, leaving organizations exposed during live disruption events.



Key findings

1	**Financial impact from disruption is consistent and material.** Organizations report an average of 2.42% revenue loss from past disruptions, with 2.65% at risk in a critical supplier outage scenario. This establishes disruption as a recurring earnings issue, not an isolated event.
2	**Visibility is concentrated at Tier 1 and Tier 2.** While 72% monitor Tier 1 and Tier 2 suppliers, only 12% extend visibility to Tier 3+, leaving upstream risk largely unmanaged.
3	**Detection happens too late to shape outcomes.** Disruptions take an average of 8.7 hours to detect, meaning organizations are identifying events as they unfold, not as they build.
4	**Financial impact is understood too slowly.** It takes 40.9 hours to quantify revenue, margin, and working capital exposure, creating a multi-day gap between signal and decision.
5	**Detection and decision-making are disconnected.** Organizations can identify disruption signals, but lack integrated systems to translate those signals into immediate, actionable decisions.
6	**Signals do not trigger coordinated action.** While 27% rely on automated alerts, only 28% report automated workflows, indicating that detection does not consistently lead to execution.
7	**Decision-making remains manual and fragmented.** A significant proportion of organizations rely on manual or semi-integrated processes, slowing response during time-sensitive disruption events.
8	**Governance does not ensure execution.** Although 40% report defined metrics and accountability, only 31% have modeled multi-supplier playbooks, showing a gap between oversight and readiness.
9	**Detection is often triggered by operational impact.** Internal analysis and operational or customer signals remain key triggers, indicating that disruption is often identified after impact begins.
10	**The system is reactive by design.** Across detection, quantification, and execution, organizations are structured to respond after disruption occurs, rather than intervene early to prevent impact.

KEY FINDING 1

Disruption is a recurring earnings event, not a one-off shock

Organizations are not dealing with isolated supply chain failures. Disruption is a consistent driver of revenue loss and ongoing financial exposure.

Lost:

2.45%

Average annual revenue lost due to supply chain disruption

At risk:

2.65%

Revenue at risk from a 30-day outage at a critical supplier

Average impact across surveyed CFOs and COOs

Supply chain disruption is not a rare event, it is a recurring source of financial impact. Organizations report an average loss of **2.42% of annual revenue**, with a further **2.65% at risk** in the event of a critical supplier outage. This indicates that disruption is not only frequent, but also predictable in its financial consequences.

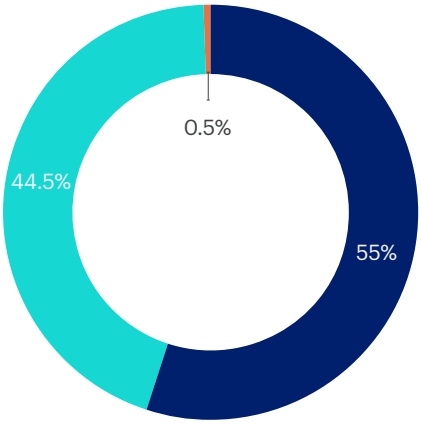
What this means

Disruption is already impacting earnings, not just operations

Exposure levels are consistent across both realized and modeled scenarios

Financial risk is measurable, but not actively mitigated at source

Question:
In the past 3 years, to what extent, if at all, has your organization experienced a supplier disruption or supply chain disruption that directly reduced revenue or halted production?



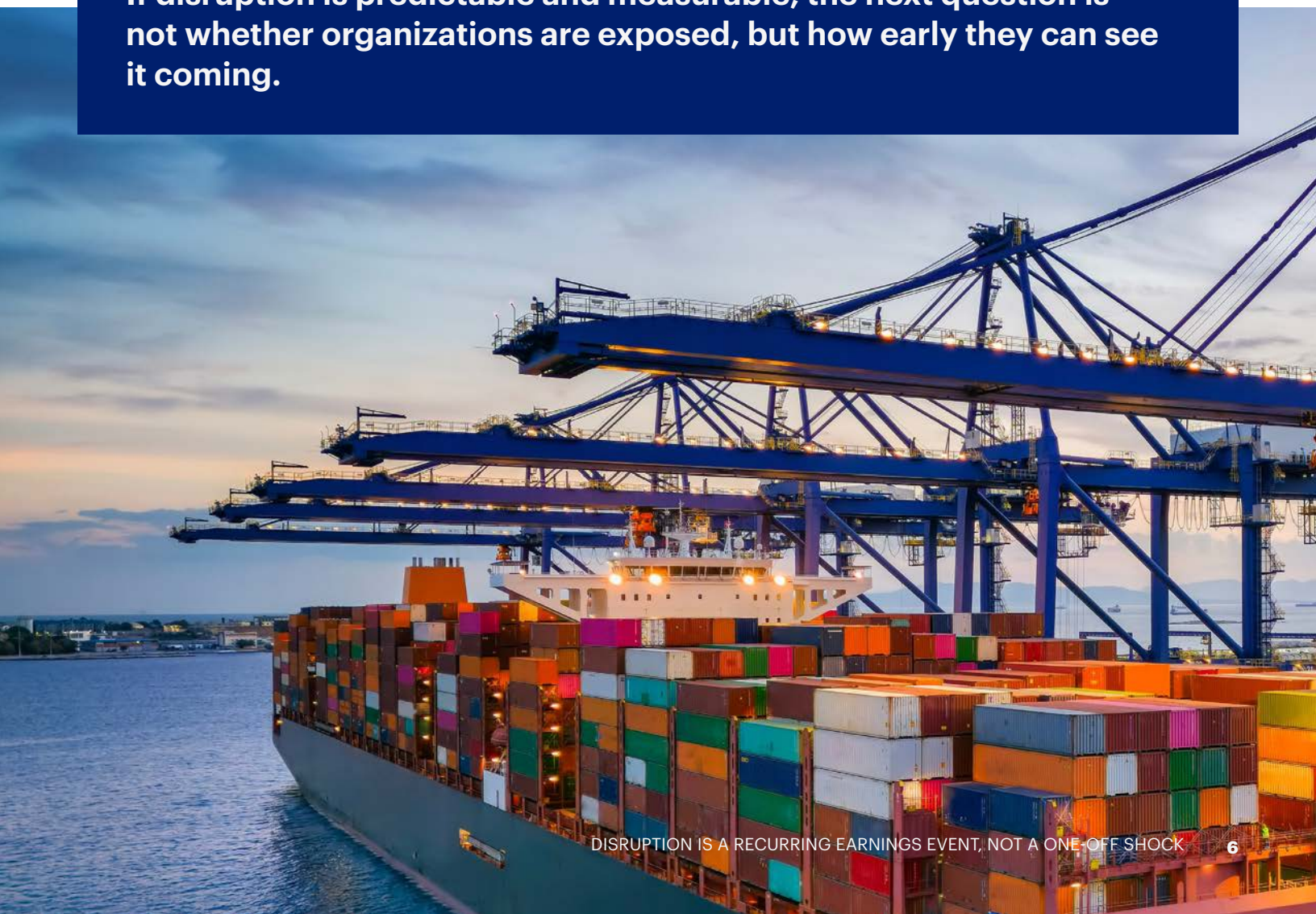
- A financial impact between 1-2% of total annual revenue
- A financial impact of between 3-4% annual revenue
- We did not quantify the financial impact

The gap

Organizations can quantify disruption impact, but only after it occurs or once a scenario is modeled. This creates a system where financial exposure is understood, but not prevented.

Key Takeaway:

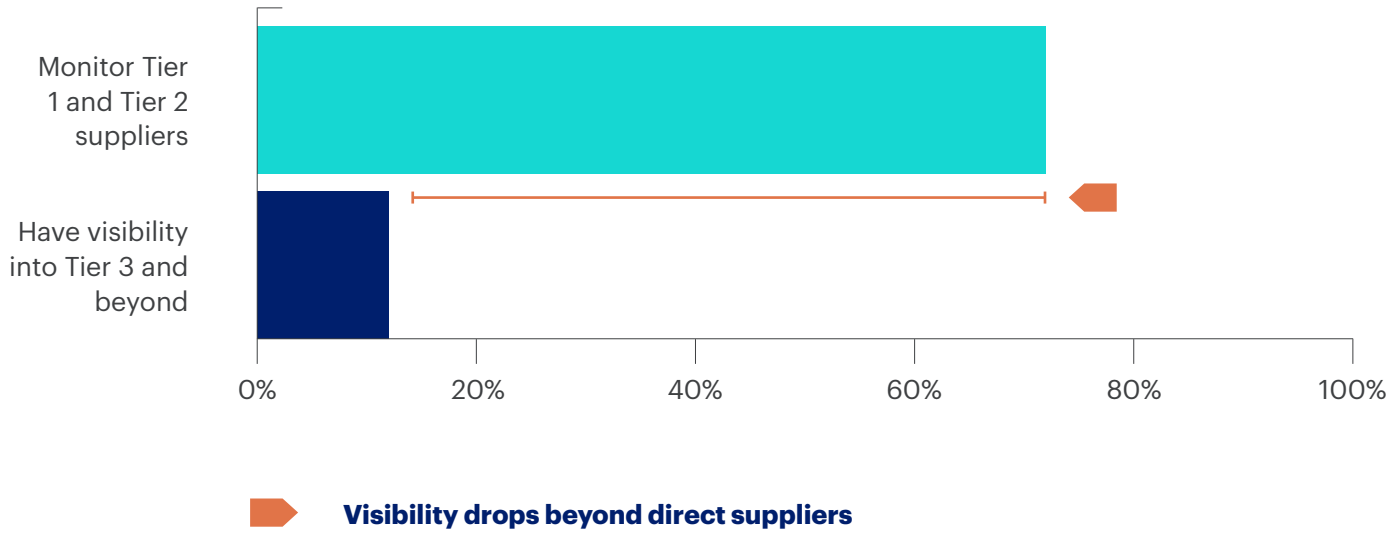
If disruption is predictable and measurable, the next question is not whether organizations are exposed, but how early they can see it coming.



KEY FINDING 2

Visibility stops where risk begins

Organizations have visibility into direct suppliers, but lack insight into the upstream network where disruption often originates.



Most organizations have established monitoring across Tier 1 and Tier 2 suppliers. However, visibility declines sharply beyond this point, with only **12% extending insight into Tier 3 and deeper**. This creates a structural blind spot, as many disruptions originate upstream before cascading through the supply chain.

What this means

Visibility is concentrated where control is highest, not where risk originates

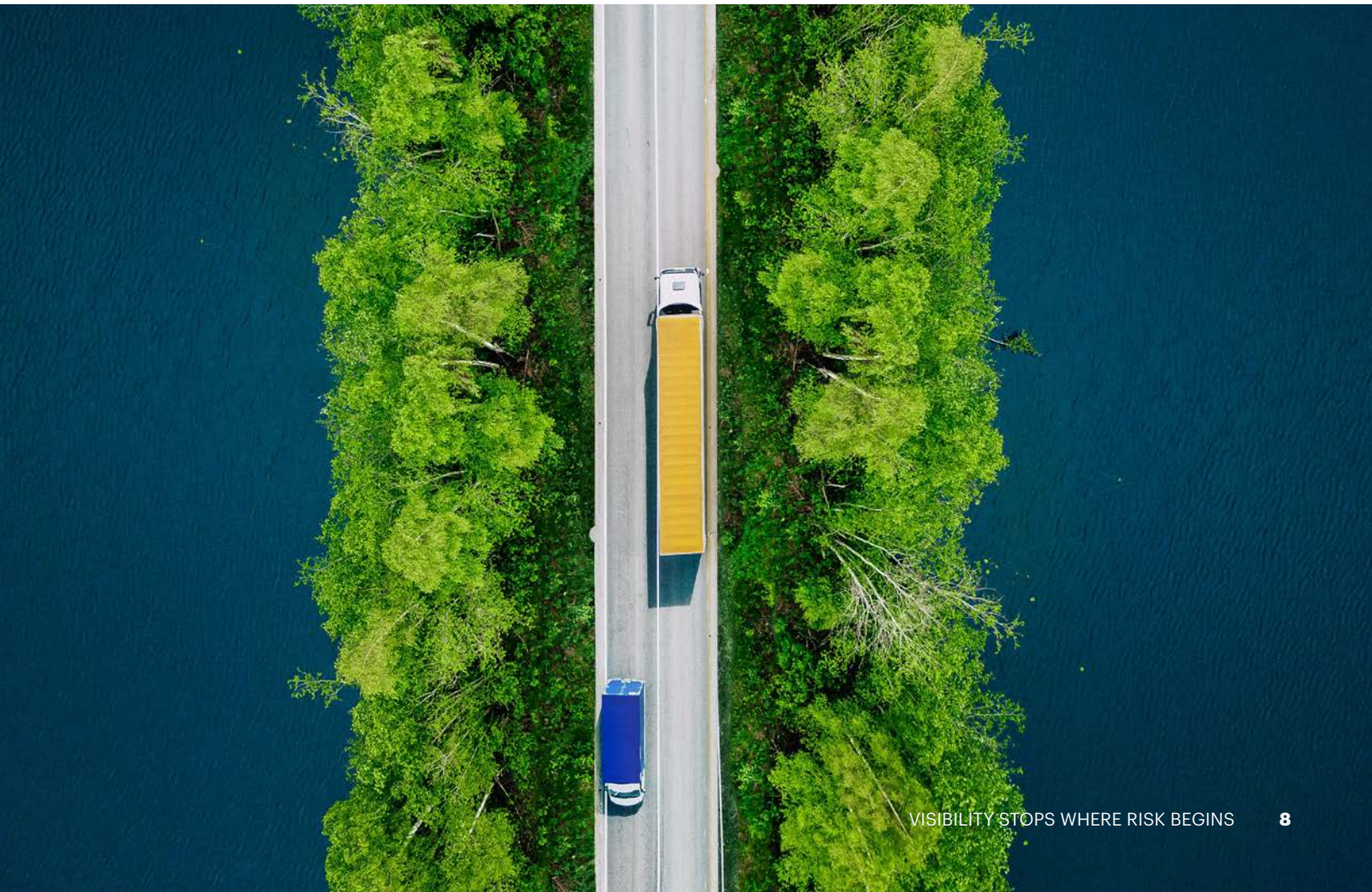
Upstream dependencies remain largely unmonitored

Organizations are exposed to disruption signals they cannot see

Key Takeaway:

Organizations believe they have visibility, but that visibility does not extend far enough to detect risk early.

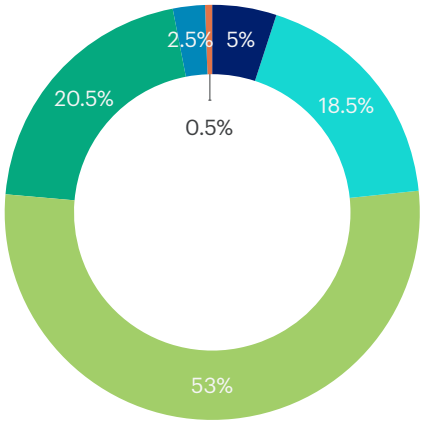
TIER 2-*N* OPACITY IS STILL LIMITED



KEY FINDING 3

Disruption is detected as it happens, not as it builds

Organizations are identifying disruption signals too late to intervene, limiting their ability to prevent operational and financial impact.



Question:
If a supplier or supply chain disruption begins, how much time, if any, does it typically take before your organization becomes aware of it?

- Immediately
- In less than 1 hour
- Within 1-11 hours
- Within 12-24 hours
- Within 2–3 days
- Within 4–7 days
- More than a week later

Risk emerges → **8.7 hour gap** → **Disruption detected**

Detection occurs during impact, not before

Organizations take an average of **8.7 hours to detect a disruption**, indicating that risk is typically identified as events unfold rather than as early signals emerge. During this time, disruptions continue to develop, reducing the ability to intervene before operational and financial consequences begin.

What this means

- **Detection is reactive, not predictive**
- **Early warning signals are not consistently captured or surfaced**
- **Response begins after disruption has already started**

27%

Rely on automated monitoring alerts as the fastest trigger

Even where automated monitoring exists, it is not the dominant detection mechanism. A significant proportion of organizations still rely on internal analysis or operational signals, reinforcing a reactive detection model.

The gap

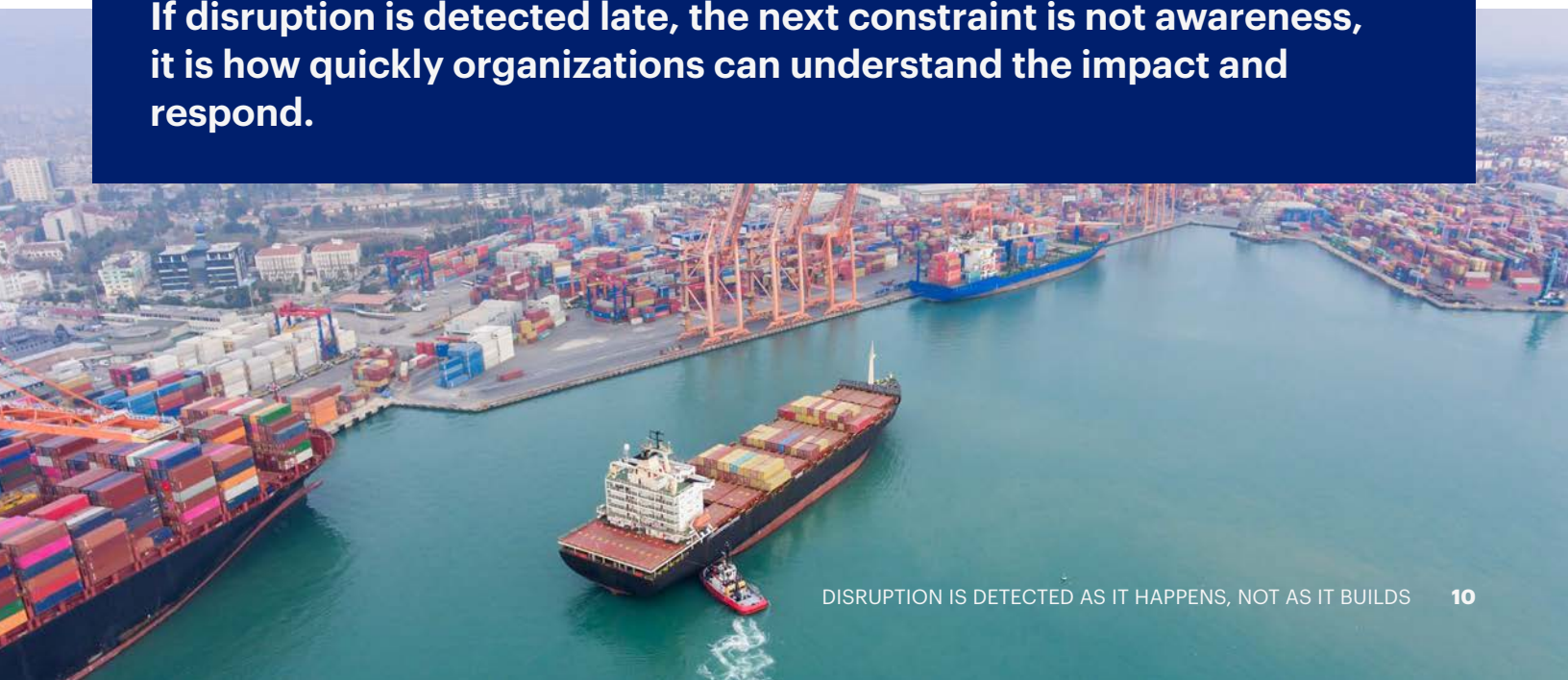
Organizations are not lacking signals, they are lacking systems that surface those signals early enough to act.

Early signal detection

Operational impact detection

Key Takeaway:

If disruption is detected late, the next constraint is not awareness, it is how quickly organizations can understand the impact and respond.



KEY FINDING 4

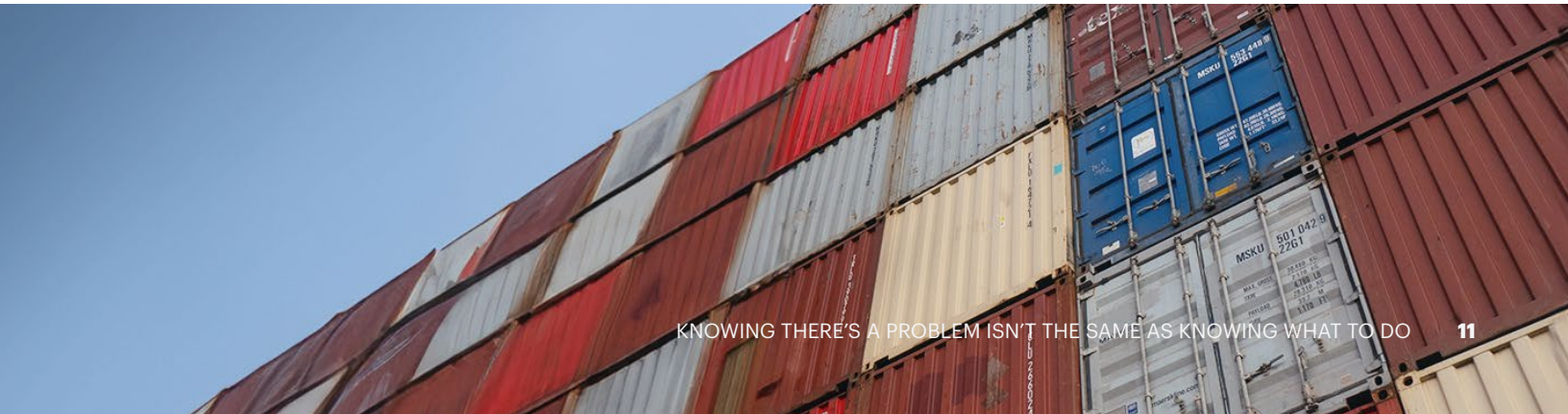
Knowing there's a problem isn't the same as knowing what to do

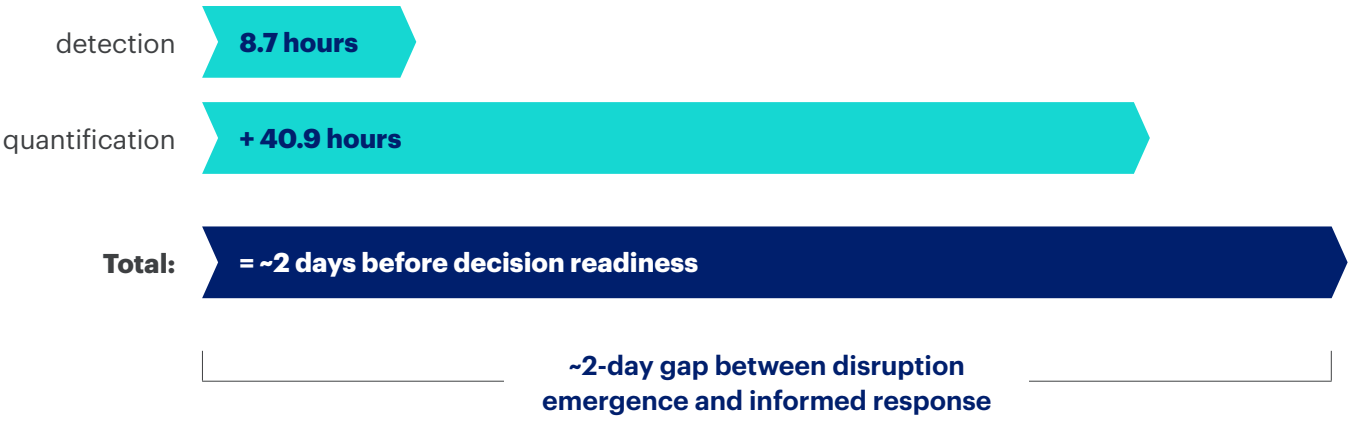
After detecting a disruption, organizations still require significant time to understand its financial and operational impact, delaying effective response.

Even after a disruption is detected, organizations require an average of **40.9 hours** to quantify its impact across revenue, margin, and working capital. This creates a prolonged delay between awareness and decision readiness, during which disruptions continue to escalate and response options narrow.

What this means

- **Detection does not enable immediate decision-making**
- **Financial and operational impact is not pre-modeled or readily accessible**
- **Teams are forced to choose between acting without clarity or waiting too long**





The gap

Organizations can detect disruption, but cannot quantify its impact fast enough to act while it is still preventable.

62%

Only occasionally model financial scenarios

Scenario modeling exists, but is not embedded into real-time decision workflows, limiting its usefulness during live disruption events.

27%

Routinely model scenarios

Pre-modeled, instant decision

Ad hoc analysis over time

Key Takeaway:

If it takes nearly two days to detect and understand disruption, the remaining question is whether organizations can execute a coordinated response in time.

KEY FINDING 5

Signals don’t trigger action

Organizations can detect and analyze disruption, but lack systems that convert insight into immediate, coordinated response.

28%

Have automated workflows triggered by risk signals

Risk signal detected → **Decision required** → **Action triggered**

Manual intervention required

While organizations are increasingly able to detect disruption signals, only **28% report that these signals automatically trigger response workflows**. This indicates that the majority of organizations still rely on manual coordination to initiate action, slowing response times and increasing variability during disruption events.

31%

Automated workflows

29%

Integrated but manual

23%

Separate systems / fully manual

What this means

- **Detection and execution are not connected**
- **Response depends on human coordination under time pressure**
- **Systems support visibility, not action**

The gap

Organizations can see disruption and understand its impact, but cannot consistently trigger the right actions at the right time.

Signal → automatic action

Signal → analysis → meetings → action

Current state is delayed and fragmented

Key Takeaway:

If action is not triggered automatically, outcomes depend on governance, consistency, and preparedness across the organization.

KEY FINDING 6

Governance exists. Execution still fails.

Organizations have introduced oversight and accountability for supply chain risk, but lack the operational systems to enforce consistent response.

40%

Have defined metrics and accountability for supplier risk

Many organizations have established governance structures for supply chain risk, with **40% reporting defined metrics and accountability**. However, this oversight does not consistently translate into action. Without systems that link governance to execution, response remains dependent on manual processes and individual decision-making during disruption events.

31%

Have modeled multi-supplier playbooks

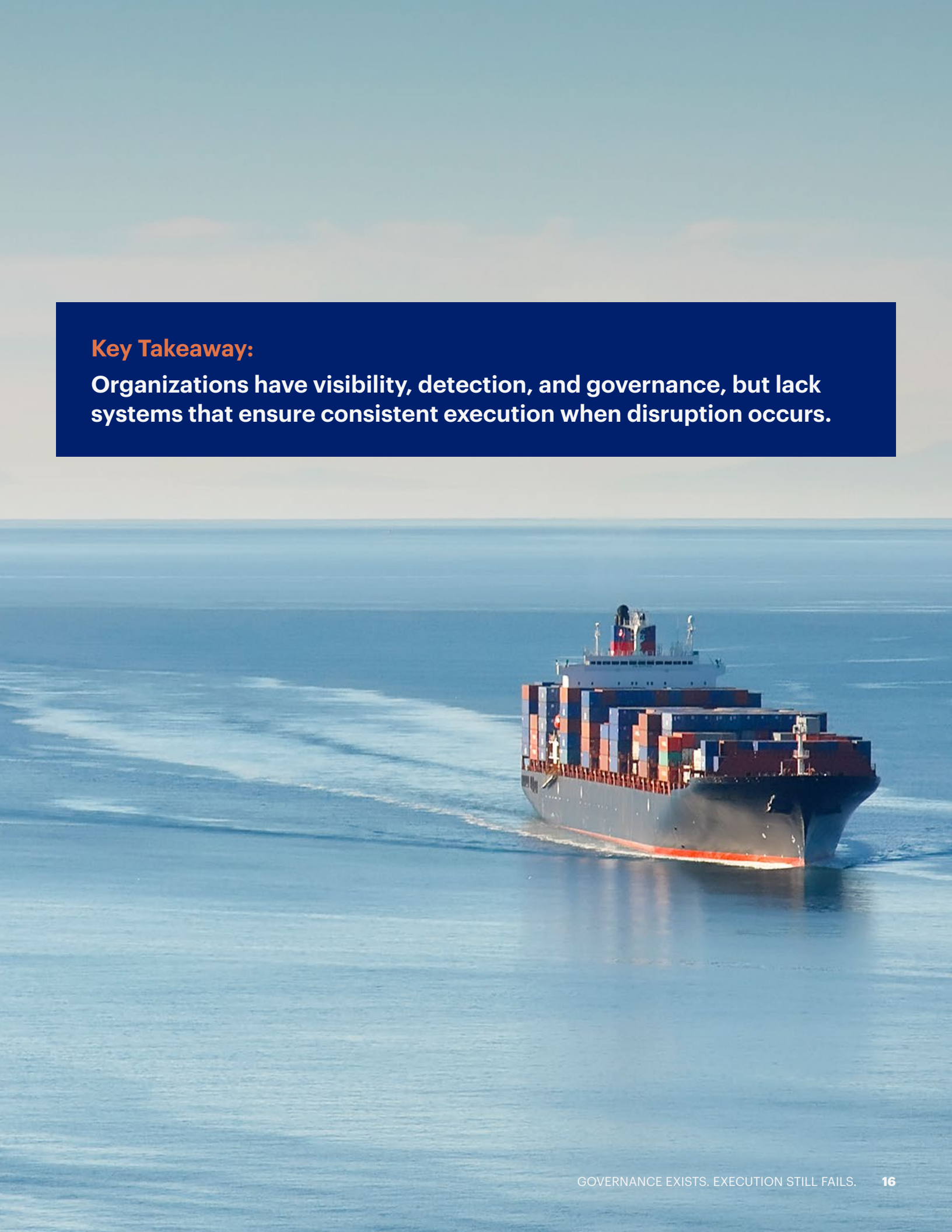
While some organizations have developed response playbooks, coverage remains limited and execution is not consistently enforced across teams or disruption scenarios.

What this means

- **Governance defines responsibility, but does not ensure action**
- **Playbooks exist, but are not consistently applied**
- **Execution varies depending on teams, timing, and context**

Key Takeaway:

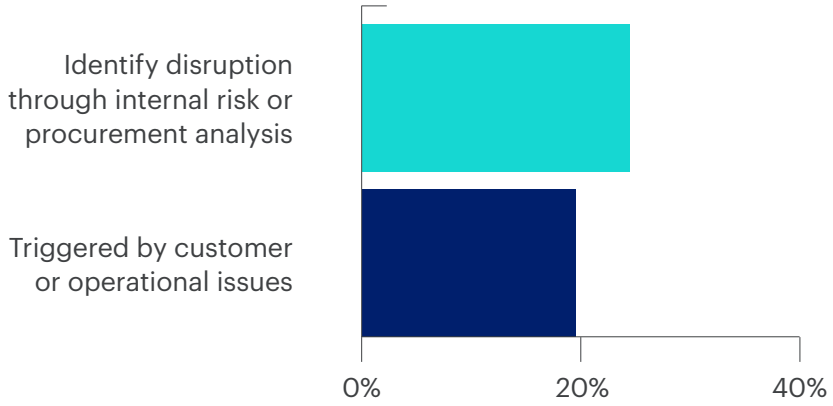
Organizations have visibility, detection, and governance, but lack systems that ensure consistent execution when disruption occurs.



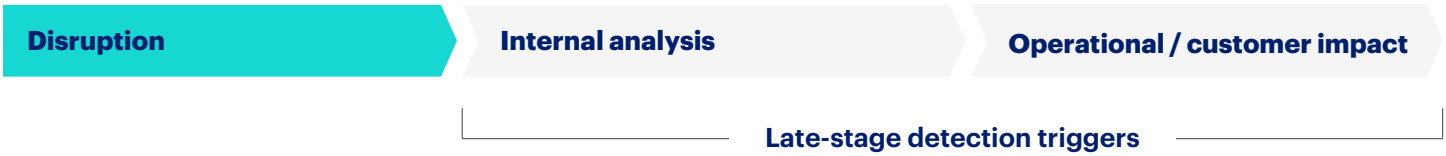
KEY FINDING 7

Disruption is identified through impact, not early signals

Organizations often become aware of disruption through internal analysis or operational issues, rather than continuous, automated signal detection.



Disruption is most commonly identified through internal analysis (**24.4%**) or after operational and customer issues emerge (**19.5%**). This indicates that detection is frequently triggered by investigation or visible impact, rather than continuous monitoring of early risk signals across the supply chain.



27%

Report automated monitoring alerts as the fastest detection trigger

Even where automated monitoring exists, it is not the dominant detection mechanism. Organizations continue to rely on human-driven analysis and downstream signals, reinforcing a reactive detection model.

What this means

- **Detection is initiated by investigation, not system alerts**
- **Operational impact is often the first visible signal**
- **Early warning capability is limited or underutilized**

The gap

Organizations are not consistently detecting risk as it emerges, only after it becomes visible through internal analysis or operational disruption.

SIGNALS ARE NOT SURFACED EARLY

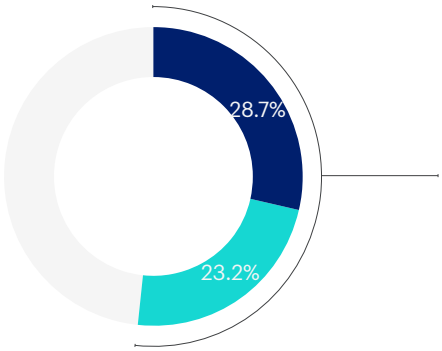
Key Takeaway:

If detection is triggered late and action is manual, the system is structurally reactive, not designed to prevent disruption.

KEY FINDING 8

Decisions are made across disconnected systems

Even when disruption is detected and understood, decision-making is fragmented across tools, teams, and workflows, slowing coordinated response.



51.9% rely on manual or semi-integrated decision workflows

- integrated but manual
- separate/manual

A majority of organizations rely on **manual or semi-integrated workflows (51.9%)** to manage disruption response. This means that detection, analysis, and decision-making are not connected within a single system, requiring coordination across multiple tools and teams. As a result, response is slowed and consistency is reduced during time-critical events.

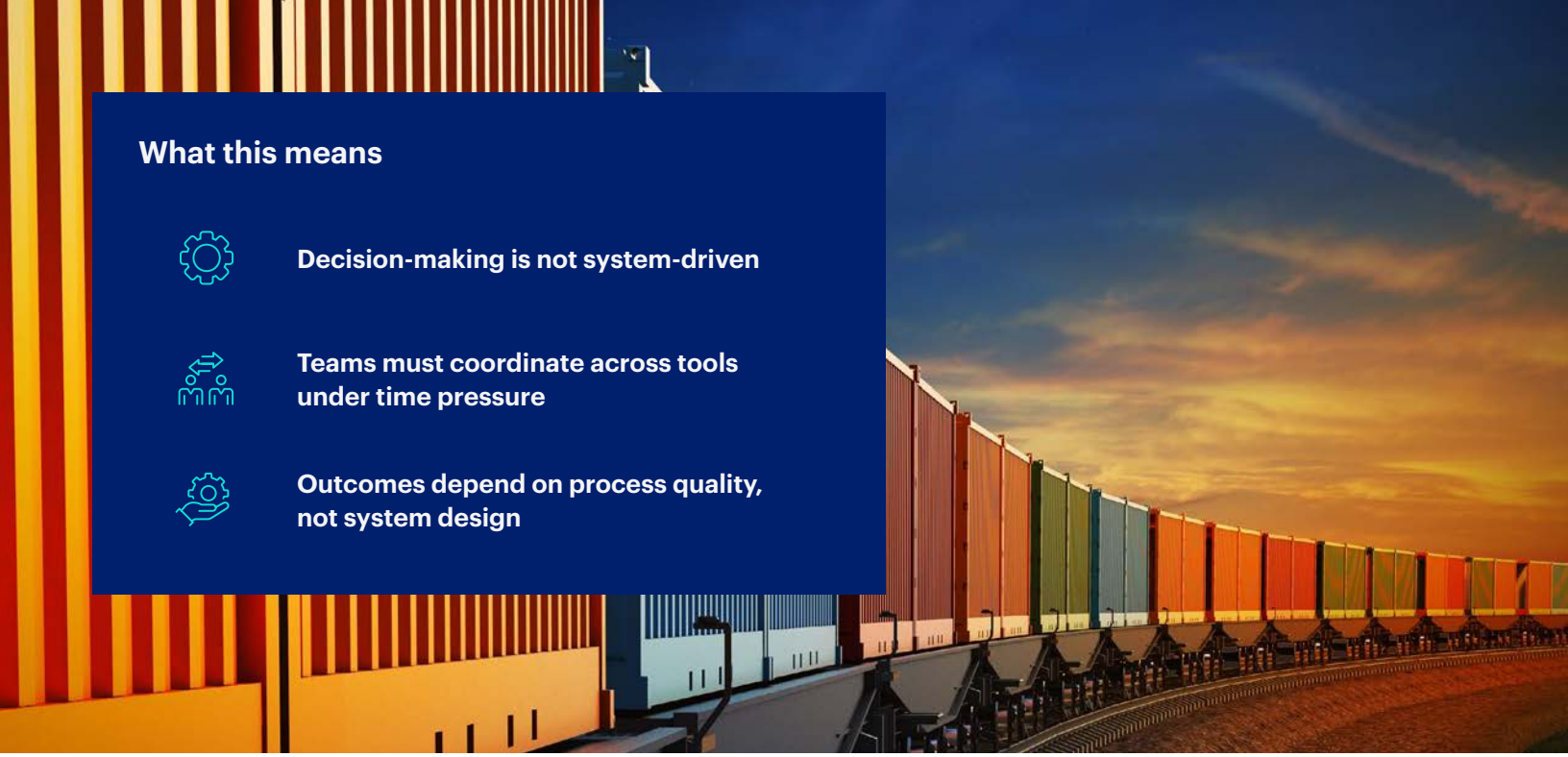
23%

Separate systems and fully manual workflows

29%

Integrated systems, but manual decision-making

Even where systems are integrated, decision-making still depends on manual input. Fully disconnected environments further increase delay and variability in response.



What this means

- Decision-making is not system-driven
- Teams must coordinate across tools under time pressure
- Outcomes depend on process quality, not system design

The gap

Organizations have systems for visibility and analysis, but lack a unified system for decision and execution.

Unified system

Fragmented system

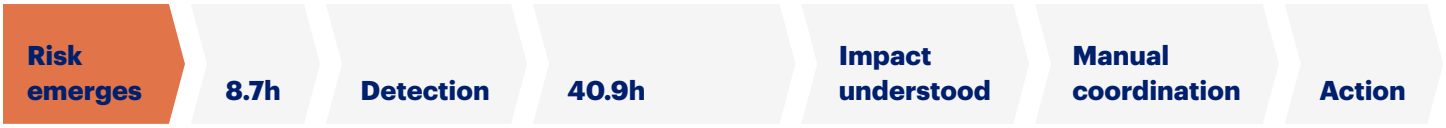
Key Takeaway:

If decision-making is fragmented, organizations cannot respond consistently, even when they have visibility, detection, and governance in place.

KEY FINDING 9

The system is reactive by design

Across detection, decision-making, and execution, organizations are structured to respond after disruption occurs, not before.



The data shows a consistent pattern across the disruption lifecycle. Risk is identified after it begins, impact takes time to quantify, and response depends on manual coordination across fragmented systems. These delays are not isolated issues, they are embedded across the entire operating model, creating a system that reacts to disruption rather than preventing it.

The compound delay

- **8.7 hours** to detect disruption
- **40.9 hours** to quantify impact
- Additional delay to coordinate and execute response

Result: A multi-day gap between disruption emergence and effective action

What this means

Prevention is structurally limited

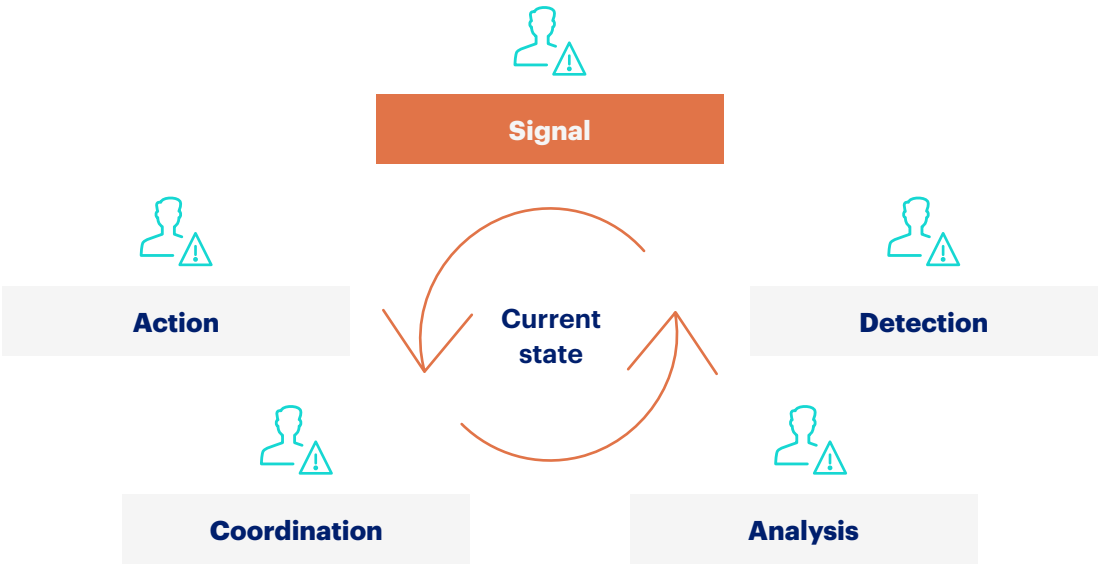
Response begins after impact is already underway

Outcomes are shaped by delay, not decision quality

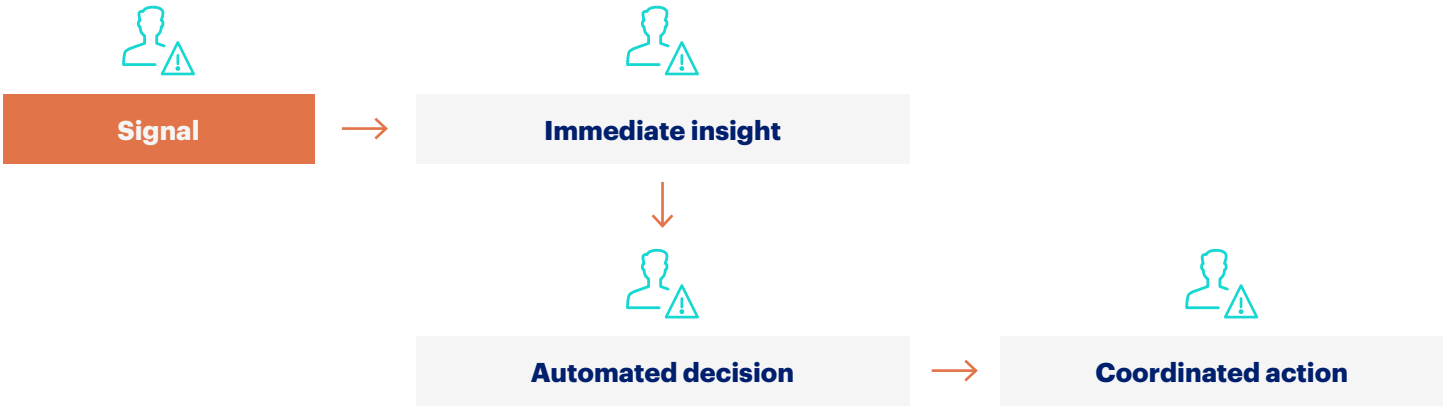
The gap

Organizations are optimizing parts of the process, but the system as a whole remains reactive.

BEFORE



AFTER



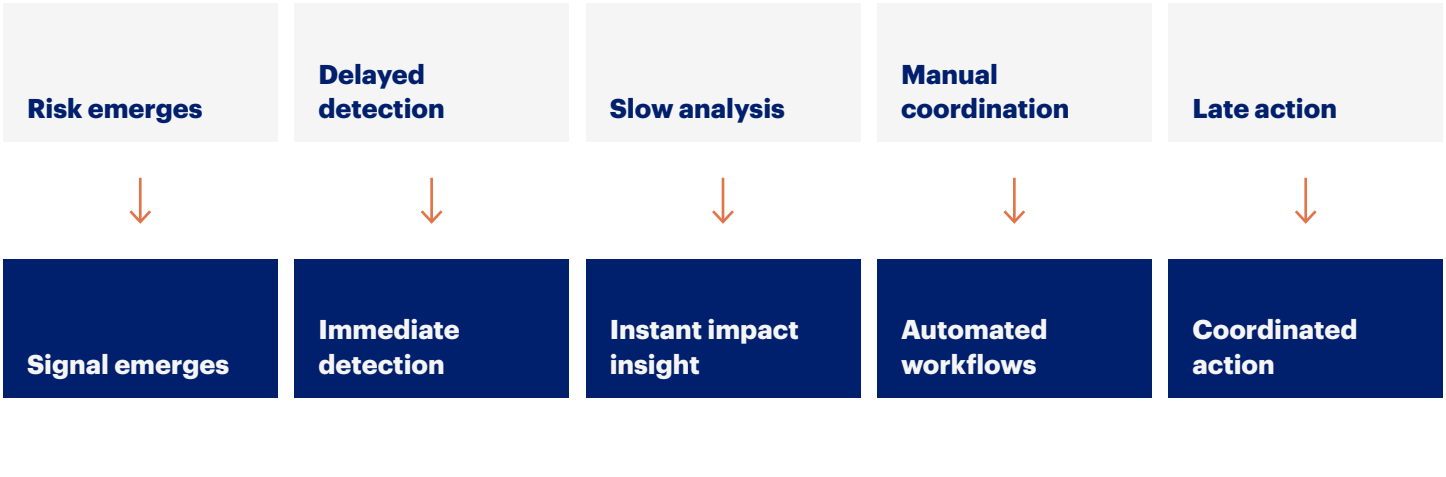
Key Takeaway:

If the system is reactive by design, the only path forward is to redesign how organizations detect, decide, and act on risk.

KEY FINDING 10

From reactive response to decision-ready execution

Closing the gap between detection and action requires a fundamental shift in how organizations operate, from fragmented workflows to connected, decision-driven systems.



The findings across this research point to a consistent conclusion: supply chain risk is not constrained by a lack of data, but by the inability to act on it in time. Organizations must move beyond monitoring and analysis toward systems that enable earlier detection, faster decision-making, and coordinated execution.

This requires connecting risk signals, financial and operational impact, and response workflows into a single, integrated system. Without this, delays will persist and disruption will continue to translate into avoidable financial and operational loss.

Sphera's Operational Intelligence platform is designed to close this gap by enabling organizations to:

- **Detect risk earlier** through continuous monitoring and AI-driven signal identification
- **Quantify impact instantly** across revenue, margin, and operations
- **Trigger coordinated response** through integrated workflows and automation

This shifts supply chain risk management from reactive response to proactive, decision-ready execution.

MAKE INTELLIGENCE DECISIONS IN-TIME

Signal	Decision	Action	Outcome
Risk signal detected	Impact automatically quantified	Workflow triggered	Action executed across teams

The shift

From:
- Visibility without action
- Detection without timing advantage
- Governance without execution

To:
- Early signal detection
- Immediate decision readiness
- Coordinated, automated response

What this means

Decisions move from hours and days to near real time

Response becomes consistent and system-driven

Financial and operational impact can be reduced before disruption escalates

Key Takeaway:

The organizations that will outperform in volatile supply environments are not those with the most visibility, but those that can act on risk first. Building that capability requires more than incremental improvement, it requires a system designed for speed, coordination, and execution.

CONCLUSION

Adopt a system that connects signal → decision → action in real time.

Organizations are not failing to detect disruption. They are failing to act on it in time.

The data shows a consistent pattern: detection is delayed, impact takes hours to quantify, and response depends on manual coordination. The result is a multi-day gap between risk emergence and effective action.

This is not a visibility problem. It is a system design problem.

Closing this gap requires more than incremental improvement. It requires a shift from fragmented workflows to a unified system that connects signals, financial impact, and execution.

The organizations that outperform will not be those with more data, but those that can move decisions earlier and execute faster.

SCRM by Sphera

Sphera is the leading Operational Intelligence Platform unifying risk, safety and sustainability insights into actionable intelligence that drives enterprise performance. Powered by Sphera AI, our platform integrates operational insights across EHS, sustainability, product stewardship, process safety and supply chains – providing enterprise-wide visibility, control and resilience that turns uncertainty into opportunity. We have served 8,500 customers and over one million users in 100 countries to help companies keep their people safe, their products sustainable and their operations productive.

Learn more about Sphera at **sphera.com.**

Follow Sphera on **LinkedIn.**

For more information contact us at:
sphera.com/contact-us

sphera®