insights

Business Continuity Planning

Lessons from Regional Disruptions in Logistics & Supply Chains



2026

When Disruption Becomes the Business Environment

Regional logistics disruptions, supply chain constraints, cyber incidents, and increasing dependence on critical third parties have fundamentally changed today's business environment. Disruption is no longer an occasional event, it is an ongoing business reality that directly affects operations, financial performance, customer confidence, and regulatory compliance.

These events have demonstrated that organizations rarely fail because disruption occurs. They struggle because disruption exposes weaknesses that already exist, including fragmented decision-making, limited visibility over critical operations, supplier concentration, and continuity plans that have never been tested.

As recognized by ISO 22301, Business Continuity Management is more than a documented plan. It is a management system that integrates governance, risk management, Business Impact Analysis, testing, and continual improvement to strengthen organizational resilience.

Business Continuity Planning has therefore evolved from a compliance requirement into a strategic capability that enables organizations to protect critical operations, maintain stakeholder confidence, and sustain business performance during uncertainty.

Disruption by the Numbers: The Saudi Context

The shift is measurable. Since regional hostilities escalated on 28 February 2026 and the Strait of Hormuz became effectively closed to container shipping, trade flows into and out of the Gulf have been re-routed at speed. Saudi Arabia sits at the centre of that shift: its Red Sea ports have absorbed diverted cargo, while Saudi-linked businesses account for **6.51%** of the more than **44,000** companies worldwide that had at least one shipment exposed by March 2026, the third-largest national share after China and the UAE.



Table 1: Gulf Trade Disruption in 2026 — Key Indicators

Indicator	Data	Source
Persian Gulf import bookings (weekly TEU)	62,935 (21–27 Feb) 18,663 (–70%, first week after 28 Feb) 5,395 (–91%, 16–22 Mar)	Dun & Bradstreet
Cancelled import bookings (TEU)	17,374 97,897 (+463%), 28 Feb–6 Mar versus 21–27 Feb	Dun & Bradstreet
Saudi Red Sea ports: import bookings (weekly TEU)	13,569 22,861 (+68%)	Dun & Bradstreet
Saudi Red Sea ports: export bookings (weekly TEU)	10,396 19,323 (+86%)	Dun & Bradstreet
Lost volume recovered through alternative routes (Saudi Red Sea and Omani ports)	50–60% of lost exports, but only about 20% of lost imports	Dun & Bradstreet (estimate)
Added transit time from Cape of Good Hope diversions	+10 to 14 days	Dun & Bradstreet
China–Jeddah spot rate per 40-ft container (FEU)	US$10,870 (≈ SAR 40,800), up 256% since 28 Feb (as of 10 Sep 2026)	Xeneta
Disrupted businesses with fewer than 50 employees	About 80%	Dun & Bradstreet

Sources: *Dun & Bradstreet maritime container booking data (published 17 July 2026); Xeneta Weekly Ocean Container Shipping Market Update (10 September 2026). TEU = twenty-foot equivalent unit; FEU = forty-foot equivalent unit. SAR converted at the fixed peg of SAR 3.75 per US$.*

The planning implication is clear: alternative routes recovered only about one-fifth of lost import volume, so re-routing alone is not a continuity strategy. Inventory buffers, pre-qualified secondary suppliers, and rehearsed decision protocols determine who keeps operating. The stakes rise further as the Kingdom scales its logistics ambitions under Vision 2030.

Table 2: Logistics in the Vision 2030 Agenda — Why Continuity Matters

Indicator	Baseline / Latest	2030 Target
Transport and logistics contribution to GDP	6% (2021)	10%
World Bank Logistics Performance Index rank	55th (2018) 38th (2023)	Top 10 globally
Annual national port container capacity	Jeddah Islamic Port expanded from 2.5m to 6.2m containers (US$270m programme, 2024)	More than 40 million containers
Logistics zones	—	Dun & Bradstreet
Sector contribution to annual non-oil revenue	50–60% of lost exports, but only about 20% of lost imports	Dun & Bradstreet (estimate)
Added transit time from Cape of Good Hope diversions	+10 to 14 days	59 zones

Sources: *Ministry of Transport and Logistics Services (MOTLS) and National Transport and Logistics Strategy announcements; World Bank Logistics Performance Index 2023; AGBI citing the Saudi Ports Authority (Mawani), April 2025; NIDLP Delivery Plan 2018–2020 as cited by The Business Year (2016 zone count).*

Executive Insight

The organizations that lead through disruption are not those with the most detailed continuity plans, they are the ones that make better decisions when disruption occurs.

Five Leadership Priorities for Building Resilience

1. Elevate Business Continuity to the Boardroom

Business Continuity should be integrated into corporate governance, Enterprise Risk Management (ERM), and strategic planning to ensure resilience is embedded in executive decision-making.

Leading Practices: Establish clear governance, executive accountability, and crisis decision-making protocols before disruption occurs.

Saudi Evidence: Board-level ownership is increasingly a regulatory expectation in the Kingdom rather than a choice. The SAMA Business Continuity Management Framework, in force since February 2017, is mandatory for SAMA member organizations, including all banks operating in Saudi Arabia, and is built on ISO 22301. The NCA's Essential Cybersecurity Controls (ECC-2:2024) require government bodies and critical national infrastructure operators to address cybersecurity resilience within business continuity management. Globally, **45.4%** of organizations now have a dedicated resilience lead reporting directly to the board, and **65.5%** report increased financial or resource support for continuity and resilience (BCI, 2025).



Table 3: Saudi Regulatory Anchors for Business Continuity

Framework	Applies to	Continuity requirements
SAMA Business Continuity Management Framework (in force since 28 Feb 2017)	SAMA member organizations, including all banks operating in Saudi Arabia and subsidiaries of foreign banks	Governance, business continuity policy, Business Impact Analysis, recovery time objectives (RTO), and continuity and IT disaster recovery plans; based on ISO 22301, ISO 27001, BCI and DRII good practice
NCA Essential Cybersecurity Controls (ECC-2:2024)	Government entities and private-sector entities that own, operate or host Critical National Infrastructure	Domain 3, Cybersecurity Resilience: subdomain 3-1 covers cybersecurity resilience aspects of Business Continuity Management
ISO 22301:2019	Any organization (voluntary, certifiable standard)	Management system covering governance, risk assessment, Business Impact Analysis, strategy, exercising and performance evaluation

Sources: *SAMA Rulebook (Business Continuity Management Framework); NCA ECC-2:2024 implementation guide; ISO 22301:2019; BCI Continuity and Resilience Report 2025.*

2. Strengthen Supply Chain Resiliencet

Recent regional disruptions have highlighted the importance of understanding critical suppliers, logistics partners, and operational dependencies.

Leading Practices: Assess supplier concentration, diversify sourcing strategies, and continuously monitor third-party resilience.

Saudi Evidence: Supply chain concentration is now a measurable exposure. Third-party and supply chain compromise was the most common initial breach vector in the Middle East, at **17%** of incidents and an average of **SAR 29.6 million** per breach (IBM, 2025). On the physical side, small and micro-businesses, which often lack buffers and alternative suppliers, make up about **80%** of disrupted entities, and wholesale trade and transportation services together account for about **46%** of impacted businesses (Dun & Bradstreet, 2026).

Table 4: Supply Chain and Third-Party Exposure Indicators

Indicator	Data	Source
Third-party or supply chain compromise as initial breach vector (Middle East)	62,935 (21–27 Feb) 18,663 (–70%, first week after 28 Feb) 5,395 (–91%, 16–22 Mar)	IBM, 2025
Sectors most affected by the 2026 Gulf disruption	17,374 97,897 (+463%), 28 Feb–6 Mar versus 21–27 Feb	Dun & Bradstreet, 2026
Fuel as a share of trucking operating costs	13,569 22,861 (+68%)	Dun & Bradstreet, 2026
Organizations that report on supply chain disruptions (global)	10,396 19,323 (+86%)	BCI, 2023
Likelihood that a supplier has no mitigation measures in place (global)	50–60% of lost exports, but only about 20% of lost imports	BCI, 2023
Top management commitment to supply chain resilience rated “high” (global)	Only about one-third of respondents	BCI, 2023

Sources: *IBM Cost of a Data Breach Report 2025 (Middle East findings); Dun & Bradstreet (17 July 2026); BCI Supply Chain Resilience Report 2023.*

3. Test Readiness, Don't Assume It

Business Continuity Plans deliver value only when they have been validated through practical exercises.

Leading Practices: Conduct regular simulations and crisis management exercises to strengthen preparedness and leadership confidence.

Saudi Evidence: Untested readiness is most expensive where detection and response are slow. Saudi organizations took an average of **226 days** to identify a breach and a further **59 days** to contain it. Those needing more than 200 days to identify and contain an incident paid an average of **SAR 32 million**, against **SAR 22 million** for those that were faster. Among Saudi organizations planning additional security investment after a breach, **52%** prioritize incident response planning and testing (IBM, 2026).

Table 5: The Cost of Slow Detection and Response — Saudi Arabia

Indicator	Data	Source
Average time to identify a breach	226 days	Detection is the longest phase of the lifecycle
Average time to contain a breach	59 days	Total lifecycle of roughly 285 days
Average cost where identification and containment took more than 200 days	SAR 32m	Baseline for slow response
Average cost where identification and containment took fewer than 200 days	SAR 22m	About 31% lower than the slow-response case
Average cost with extensive use of AI and security automation versus none	SAR 23.15m versus SAR 32.08m	About 28% lower with extensive use

Sources: *IBM Cost of a Data Breach Report 2026, Saudi Arabia findings (Ponemon Institute; 602 organizations globally, March 2025–February 2026). Percentage differences are calculated from the reported averages.*

4. Integrate Business Continuity with Enterprise Risk Management

Operational disruption is closely linked to cyber risk, third-party risk, regulatory change, and technology resilience.

Leading Practices: Develop an integrated resilience framework that connects Business Continuity with Enterprise Risk Management, Governance, and Internal Audit.

Saudi Evidence: Cyber incidents are a direct source of operational disruption, and they carry a measurable price. The average data breach in Saudi Arabia costs **SAR 27 million**, rising to **SAR 38 million** in financial services and **SAR 35.4 million** in the industrial sector, and **one in four** malicious breaches is now AI-enabled. This is despite the Kingdom's strong national posture: it was classified Tier 1 ("Role-modelling") in the ITU Global Cybersecurity Index 2024 and ranked first in the IMD World Competitiveness Yearbook cybersecurity indicator in 2025. National strength does not remove organization-level exposure.

Table 6: Data Breach Cost Benchmarks — Saudi Arabia (2026)

Category	Saudi Arabia result
Overall	
Average cost of a data breach	SAR 27.0m
By sector	
Financial services	SAR 38.0m
Industrial	SAR 35.4m
Technology	SAR 33.0m
Costliest attack vectors	
Exploiting public-facing applications	SAR 34.7m
Abusing valid accounts	SAR 33.3m
Phishing, including voice and SMS phishing	SAR 30.6m
Post-breach investment intentions	
Organizations planning to increase investment in security tools and governance	62%
Of those investing: data loss prevention / incident response planning and testing / hiring skilled specialists	60% / 52% / 41%

Sources: *IBM Cost of a Data Breach Report 2026, Saudi Arabia findings. National rankings: ITU Global Cybersecurity Index 2024; IMD World Competitiveness Yearbook 2025, as reported by the National Cybersecurity Authority.*

5. Build Resilience as an Organizational Capability

Resilience is sustained through leadership, governance, awareness, and continuous improvement, not documentation alone.

Leading Practices: Embed resilience into organizational culture through training, accountability, and regular reviews.

Saudi Evidence: Culture and capability are the multiplier. More than **70%** of organizations globally now run an operational resilience programme, a record high (BCI, 2025). Yet the Saudi breach data shows where capability gaps persist: only **37%** of breached organizations encrypted sensitive data both at rest and in transit, **54%** did not, and **25%** reported no use of AI or security automation in their security operations (IBM, 2026).

The Insights Perspective

Many organizations ask:
"Do we have a Business Continuity Plan?"
A more valuable executive question is:
"Can we continue making informed decisions when the unexpected occurs?"

Business Continuity Planning should not be measured by the number of documents produced. Its success is measured by an organization's ability to protect critical operations, maintain stakeholder confidence, and recover with agility.

Measured by outcomes, resilience can be tracked through a small set of board-level indicators. Where external benchmarks exist for the Kingdom, they provide a starting reference point; the rest should be set through Business Impact Analysis.



Table 7: Board-Level Resilience Indicators and Reference Points

Indicator	What it tells the board	Reference point
Time to identify and contain a major incident	Speed of detection and response	Saudi average: 226 days to identify, 59 days to contain (IBM, 2026)
Critical services with approved and tested RTO / RPO	Whether recovery targets are defined, owned and proven	Organization-specific; set through Business Impact Analysis, as the SAMA framework expects for its members
Critical suppliers with tested continuity arrangements	Third-party concentration and resilience	Global benchmark: nearly 50% chance a supplier has no mitigation in place (BCI, 2023)
Exercise frequency and scenario coverage	Whether plans have been validated under pressure	Organization-specific; set through Business Impact Analysis
Financial exposure of a major cyber incident	Quantified downside for risk appetite discussions	Saudi average SAR 27m; SAR 38m in financial services (IBM, 2026)

Sources: *IBM Cost of a Data Breach Report 2026; BCI Supply Chain Resilience Report 2023; SAMA Business Continuity Management Framework..*

Ultimately, resilience is not an operational outcome—it is a leadership capability.



How Insights Helps Organizations Build Resilience

At Insights Financial & Management Consulting, we help organizations transform Business Continuity from a compliance obligation into a strategic business capability.

Our services include:

01 Business Continuity Maturity Assessments

02 Business Impact Analysis

03 Business Continuity Risk Assessments

04 Business Continuity Strategy and Plan Development

05 Crisis Management Frameworks and Simulation Exercises

06 Integration of Business Continuity with Enterprise Risk Management, Governance, Internal Audit, and Compliance

Our approach combines governance, risk intelligence, and operational expertise to build practical resilience frameworks aligned with business objectives and regulatory expectations.



Executive Takeaway

Organizations cannot eliminate uncertainty, but they can determine how prepared they will be to respond.

Those that invest in resilience today will be better positioned to protect critical operations, maintain stakeholder confidence, and sustain long-term performance.

The next disruption is inevitable. The real differentiator will be an organization's ability to lead through it.

Sources and Notes

- Dun & Bradstreet, "Navigating Disruptions to the Strait of Hormuz 2026" (17 July 2026).
- Xeneta, Weekly Ocean Container Shipping Market Update (10 September 2026).
- IBM, Cost of a Data Breach Report 2026, Saudi Arabia findings (3 August 2026); Cost of a Data Breach Report 2025, Middle East findings (30 July 2025).
- Business Continuity Institute (BCI), Continuity & Resilience Report 2025; Supply Chain Resilience Report 2023.
- Saudi Central Bank (SAMA) Rulebook, Business Continuity Management Framework (in force 28 February 2017).
- National Cybersecurity Authority (NCA), Essential Cybersecurity Controls ECC-2:2024 and implementation guide; ITU Global Cybersecurity Index 2024; IMD World Competitiveness Yearbook 2025.
- Ministry of Transport and Logistics Services, National Transport and Logistics Strategy announcements; World Bank Logistics Performance Index 2023; AGBI (April 2025) citing the Saudi Ports Authority.

Figures reflect publicly available data as of 15 October 2026. Regional trade data from early in the 2026 disruption (March) is a snapshot and has since evolved. Global benchmarks (BCI, IBM Middle East) are shown where Saudi-specific data is not available. SAR/US$ conversions use the fixed peg of SAR 3.75.



Contacts Us

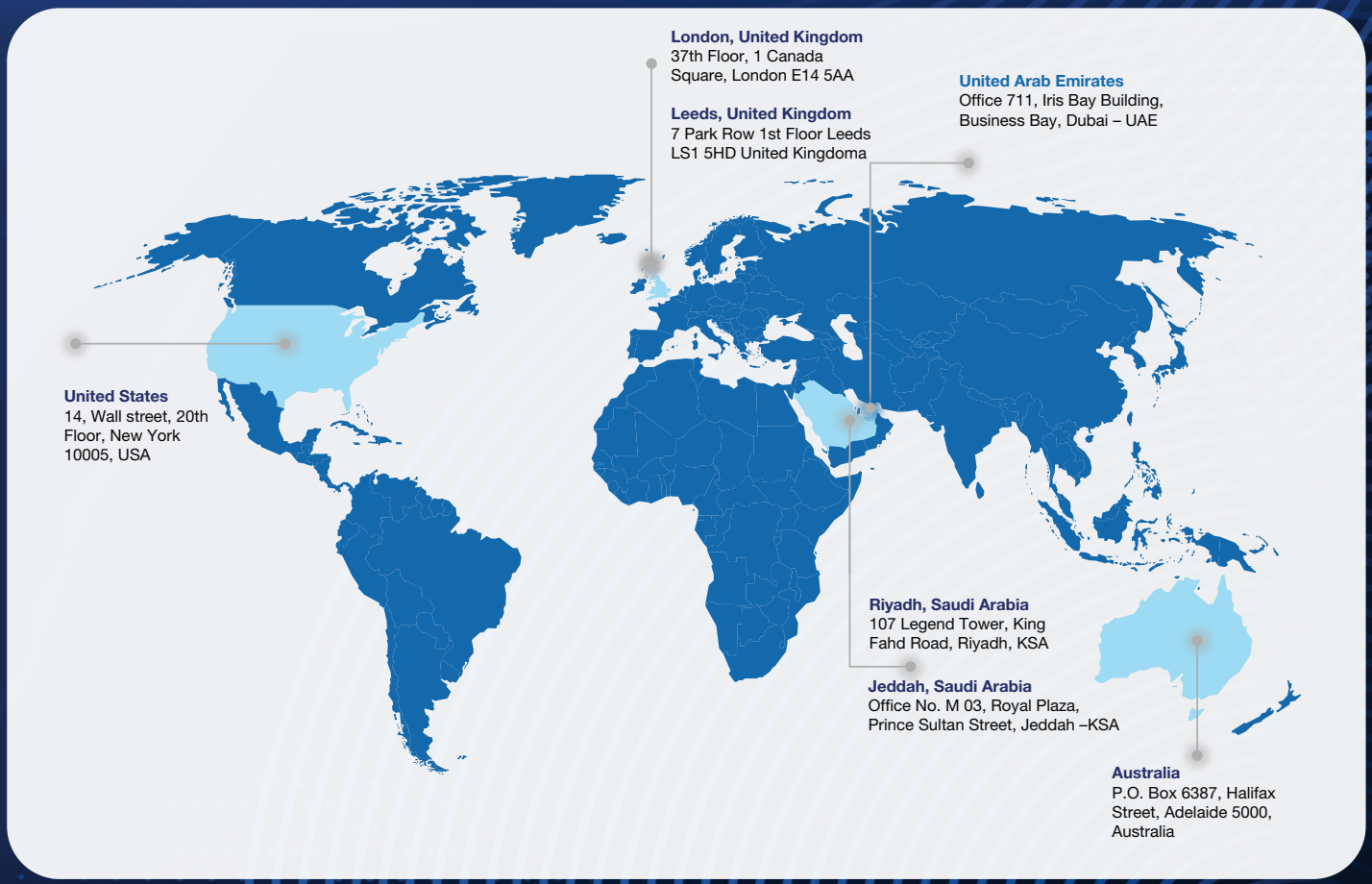
For further information, clarification and discussion concerning the contents, please contact

Khawaja Soha Butt
Partner - Financial & Risk Advisory
✉ : sbutt@insightss.co

Nick Whitford
SVP – Business Growth
✉ : nwhitford@insightss.co

Ameer Abbas
VP - Financial & Risk Advisory
✉ : aabbas@insightss.co

INTERNATIONAL FINANCE AWARDS 2021 ★★★★★
FASTEST GROWING FINANCIAL AND MANAGEMENT CONSULTANCY
SAUDI ARABIA



Insights
✆ : +966 53 775 0075
✆ : + 966 11 2930 665
✉ : info@insightss.co
🌐 : www.insightss.co

Navigating Complexity, Simplifying Success

2026

insights