First Take

# Iran War Demands Immediate Executive Action, Even If You’re Outside the Middle East

3 March 2026

First Takes like these are usually reserved for Gartner clients.
→ Contact us to learn more.

# First Take: Iran War Demands Immediate Executive Action, Even If You're Outside the Middle East

3 March 2026 - ID G00851329 - 10 min read

By: Mary Mesaglio, Trisha Rai, Vaughan Archer, David Gonzalez, Paul Catherwood, Lydia Leong, Pete Shoard, Christie Struckman, Suzie Petrusic, Elizabeth Kilbride

Initiatives: Delivery of Functional Responsibilities; Engineer Profit Amid Shifting Cost Mandates; Mobilize Leaders for Growth Amid Uncertainty; Manage Reputation Amid AI-Fueled Truth Decay; CxO Leadership; Financial; Functional Design; Strategy, Risks and Opportunities

The Iran war has significant business impact for organizations both within and outside the region. Gartner has identified critical next steps for heads of HR, IT and I&O, finance, information security, supply chain, and communications to avoid disruption and productivity loss. This is part one of a two-part series.

## C-Suite Executives Should Operate Under the Assumption That the Iran War Will Escalate

Beyond the headlines and geopolitical chatter concerning the Iran War that began on 28 February 2026, [1] there is a small set of function-specific actions that C-suite leaders must take. The safest move for executive leaders right now is to plan for conflict escalation — whether or not their enterprise operates in the Middle East.

Gartner has gathered the immediate actions for these key function heads:

- CHROs
- CIOs and heads of I&O
- CFOs
- CISOs
- CSCOs
- Chief communications officers

For part two of the series and guidance for general counsel; heads of ERM; chief procurement officers; heads of IT sourcing, procurement and vendor management; and chief marketing officers, see First Take: Executive Leaders Must Plan Ongoing Risk Mitigation for the Iran War.

## CHROs: Prioritize Protecting Employees, Clear Communication and Resilience Support

**Analysis by:** Trisha Rai

Multiple countries in the region are experiencing instability as a result of the conflict, affecting both employees in the area and employees with personal connections to the region. CHROs must prioritize workforce protection, addressing talent vulnerabilities including employees' physical safety; difficulties in relocating or evacuating staff; mental health strain due to threats of violence; and major disruptions to travel, operations and supply chains in the region. There may be additional financial impact or financial panic, adding further complexity.

Prioritize the following actions:

- **Ensure employee safety.** Activate emergency protocols, update contact information and coordinate with security teams for evacuation or shelter-in-place guidance. Deprioritize business travel to and from impacted areas until the situation stabilizes.
- **Communicate key safety information and activate crisis communication channels.** Establish ownership for crisis communications by partnering closely with leaders, managers and crisis management teams. Create dedicated channels for employees to ask questions or report changes in local conditions.
- **Prepare for operational disruption.** Identify critical roles, cross-train staff where possible, and plan for remote work or temporary reassignments as needed to maintain business continuity and minimize productivity loss. Engage the support of employees in less-affected regions.
- **Equip managers to support mental health and well-being.** Maintain workforce resilience and reduce the risk of long-term absenteeism or burnout by prioritizing individual and personal outreach through managers. Ensure that managers communicate about available resources, such as employee assistance programs, and consider equipping them with talking points that reflect consistent company values.

- **Assess employee perspectives.** Guide enterprise-level messaging by analyzing employee perspectives, mobilizing HR resources and supporting values-consistent messaging.

## CIOs and Heads of I&O: Go Beyond Disaster Recovery

**Analysis by:** Christie Struckman, Lydia Leong

CIOs must both mitigate the risks to IT capabilities and provide a single voice to executives regarding the war's impact on the enterprise technology ecosystem.

**To mitigate risks,** CIOs with workloads or data in the Middle East must take these immediate actions:

- **Urgently evacuate your critical data and applications from the Middle East,** if possible. The sooner you do this, the less contention there will be for capacity in other areas of the world. Most organizations will likely move to data centers in Europe for this purpose. Monitor for Middle Eastern governments announcing relaxation of sovereignty rules to reduce data risks.

- If evacuation is not immediately possible, **activate your disaster recovery (DR) plan.** Prepare your recovery sites to receive your workloads and data, including scaling capacity as needed. Alert the staff and third parties that will be necessary to execute a recovery.

- **Verify your secure off-site backups, and conduct tabletop recovery drills.** If you lack such backups, cloud storage can be obtained on demand and has been used to safeguard data in previous conflicts, notably by entities in Ukraine and its neighbors. Conduct ransomware-recovery and DR drills as tabletop exercises to ensure preparedness.

Regardless of geography, all CIOs must take the following actions to mitigate risk:

- Anticipate **cybersecurity attacks** and, thus, raise security operations center (SOC) monitoring levels.

- Validate your **incident response readiness** and confirm **backup immutability.**

- Scan for **navigational signal disruption** by watching GPS spoofing reports, satellite communication interference and maritime navigational anomalies.

**To provide a single voice to executives** regarding the war's impact, coordinate with your general counsel to determine who to communicate with on the board, and how. Communicate the following to the executive team to set expectations for impact:

- **Data center costs will rise** due to rising energy prices and the need to implement redundancy or failover plans if data centers are in the Middle East. Partner with your CFO regarding long-term financial impacts and strategies.
- **Procurement will be delayed** due to rerouting away from conflict areas and anticipated backlogs due to the disruption. The enterprise needs to monitor fleet movement, logistics platforms, IoT infrastructure and any aviation systems.
- **Employees in the Middle East will experience connectivity challenges.** Underwater cables have been damaged in the Red Sea, and power has been lost to three AWS data centers (affecting SASE vendors such as Zscaler) as of this writing. Time to recover is not clear.
- In the slightly longer term:
    - Sovereignty plans must be expedited if already underway. If not, support is needed to move forward with developing and implementing those plans.
    - Organizations can expect a financial impact on AI investment plans as the hyperscalers' plans involve bigger data centers (with more energy at elevated costs).

## CFOs: Focus on Balance Sheet Discipline More Than Cost Management

**Analysis by:** Vaughan Archer

Although higher oil prices may cause immediate margin compression for organizations like airlines, shippers and companies reliant on Middle East oil, for most CFOs, oil price will only be a distraction, as the global oil markets are significantly oversupplied. The true threat is the prospect of credit and insurance markets tightening, acting as a hidden tax on capital structure, regardless of whether you move physical goods or digital services. While CFOs should review all shipping and logistics contracts and analyze the impact of both a rapid ceasefire and a prolonged conflict, these operational steps are only half the equation. Ultimately, balance sheet decisions will determine your room to maneuver.

Prioritize the following actions:

- **Freeze reactive oil-price hedging.** Avoid new long-term energy or commodity contracts for 72 hours. If needed, use short-term options to cap extreme oil price spikes while preserving downside.
- **Audit your debt maturity map.** Review all maturities within the next 18 months and consider enacting preemptive revolver drawdowns or bridge facilities before lender risk appetite tightens.
- **Strengthen operational continuity.** Confirm the ability of uncompromisable backups and multiregion system distributions to withstand major utility or ISP outages that may result from Iranian cyber-strikes.
- **Establish an executive early-warning system.** Define clear triggers — such as credit-spread moves or Tier 1 provider outages — to guide capital allocation decisions.

## CISOs: Prepare for Increased Cyberattacks Independent of Physical Events

**Analysis by:** Pete Shoard

A surge in attacks from known advanced persistent threat groups is highly likely, targeting high-profile, well-known U.S.-partner-aligned infrastructure with increasingly indiscriminate methods. Iranian-affiliated cyber actors and aligned hacktivist groups frequently exploit targets of opportunity by leveraging unpatched or outdated software with known common vulnerabilities and exposures, as well as default or commonly used passwords on internet-connected accounts and devices. [2]

Common risks include availability and continuity issues resulting from ransomware or denial of service, website defacement and the leaking of sensitive information. CISOs must immediately prioritize a broad and robust resilience strategy, operationalizing effective failover procedures and aggressive infrastructure hardening in order to decisively limit risk to organizational systems and interests.

Prioritize the following actions:

- **Conduct a leadership tabletop exercise.** Test the organization's cyber defense and incident response preparedness with a leadership tabletop exercise. Examine scenarios where hacktivist groups prioritize maximum disruption, including ransomware, data theft, destructive actions and defacement.
- **Strengthen identity and** access management **(IAM).** Ensure that any on-premises IAM systems are patched with current backup and recovery processes. Immediately remediate leaked credentials; enforce multifactor authentication on all critical systems; and eliminate excessive permissions for administrative, machine and executive accounts. Increase identity threat detection to ensure that undermanaged identities, especially service accounts, are not being exploited.
- **Isolate** cyber-physical systems **(CPS) and prepare for resilience action.** Disconnect CPS (e.g., SCADA, IIoT) from the public internet unless connectivity is essential for their core functions. Where it is essential, make sure they do not have default passwords, and deploy CPS secure remote access solutions. Prepare for resilience actions, such as testing backup/recovery and incident response capabilities with production engineers. Do not delay deploying CPS protection platforms with strong threat intelligence capabilities, even if the effort is time- and resource-intensive.
- **Implement robust backup and restoration procedures.** Work with I&O leaders and business stakeholders to schedule frequent configuration backups and validate restoration processes to minimize operational disruption in the event of a security breach.

## CSCOs: Manage Disruption Without Overcommitting — Balance Increased Costs With Resilience

**Analysis by:** David Gonzalez, Suzie Petrusic

CSCOs should plan for both rapid ceasefire and prolonged conflict. Many supply chains will experience disrupted shipping lanes, conflict surcharges and tightening capacity, but CSCOs must avoid overreacting to short-term freight volatility. The real risk is the compounding impact of corridor closures, insurance constraints and rising cyber exposure, which quietly erodes continuity. Adjusting routings and stabilizing logistics will be critical, but operational moves are only half the equation; network-design and risk-governance choices will ultimately determine your room to maneuver.

Prioritize the following actions:

- **Pause reactive carrier or routing commitments.** Avoid locking into long-term freight or modal-shift agreements for now; if needed, use short-term spot capacity to cap exposure while preserving options.
- **Audit critical supply and transport dependencies.** Review Tier 1 and Tier 2 suppliers, lanes, and nodes exposed to disruption in the Red Sea and the Strait of Hormuz, and validate true alternatives.
- **Strengthen continuity in logistics and digital infrastructure.** Confirm backups for transportation systems, visibility platforms and critical operations as cyber risk increases.
- **Establish early-warning triggers.** Define clear triggers — such as war surcharges, carrier withdrawals and corridor delays — to guide changes to transportation plans, inventory allocation and C-suite communication.

## Chief Communications Officers: Trigger Crisis Management Playbook

**Analysis by:** Paul Catherwood, Elizabeth Kilbride

Even companies with no direct footprint in the region face exposure through market volatility, cyber risk, political polarization, protest activity and supply chain disruption. Chief communications officers must now shift from contingency planning to active crisis management readiness.

Prioritize the following actions:

- **Work with stakeholders to prepare structured messaging.** Prepare and preclear holding statements that cover employee safety and travel guidance, operational continuity, market volatility, cyber disruptions, and investor reassurance.

- **Have all planned external messaging reviewed for appropriateness.** Align content-producing functional leaders to review all in-flight messaging (e.g., scheduled posts and campaigns). Pause any messaging that could be read as lacking sensitivity to the current geopolitical context.

- **Clarify your social and geopolitical response framework.** Revisit guidance for when the company should speak or remain silent and who makes the final call.

- **Monitor key stakeholder concerns.** Use media monitoring and listening tools to gauge sentiment of key audiences, including investors, employees and customers.

## Contributors

Rachel Bernstein, Ron Blair, Stanton Cole, Ed Gabrys, Milind Govekar, Ramon Krikken, Alvaro Mello, Fintan Quinn, Mike Ramsey, Mary Ruddy, Mike Shevlin, Pete Shoard, Katell Thielemann, Charlie Winckless

## Evidence

[1] U.S. and Israel Attack Iran, Live Updates, The New York Times.

[2] Iranian Cyber Actors May Target Vulnerable U.S. Networks and Entities of Interest (PDF download), U.S. Cybersecurity and Infr astructure Security Agency, Federal Bureau of Investigation, the Department of Defense Cyber Crime Center and the National Security Agency.

For those with stabilized operations, the next order of business is outlined here.

Gartner has gathered the immediate actions for these key function heads:

- General counsel
- Heads of ERM
- Chief procurement officers
- Heads of IT sourcing, procurement and vendor management
- Chief marketing officers

## GC: Identify Risk Impacts and Escalate Material Information to the Board

**Analysis by:** Laura Cohn, Abbott Martin

As a strategic advisor to senior leadership, the general counsel (GC) must prepare the organization to rapidly respond to the Iran war.

Prioritize the following actions:

- **Identify the risk impacts of the event with cross-functional partners.** Work with HR, trade and supply chain, operations, finance, IT, and ERM partners to continue to identify likely impacts that require a response. For expediency, maintain a list of questions to ask for any significant geopolitical event. For the Iran war, questions should probe which contractual rights were triggered and what a changed sanctions regime means for the organization's supply chain.

- **Determine whether to escalate to the board.** To determine whether to escalate material impacts to the board, coordinate with other C-suite partners to evaluate the business impact and durability of the event. For business impact, consider how the event may change your profit margins, customer base, sales channels, operations and supply chain reliability, and talent attraction and retention, compared to your competitors'. To assess durability, consider whether the event represents a change in preceding norms and assumptions or represents a structural change in the rules of global business (e.g., trade architecture, capital mobility, technology flows, security alliances, regulatory alignment). Consider also whether the event is likely to be alleviated (by law, political turnover or other change).

- **Integrate the geopolitical risk assessment into organizational decision making.** Take steps to make sure the organization's strategic, operational and risk management decision-making processes integrate with the updated understanding of political risk. Geopolitical risk assessments should capture:
    - The impacts on strategic planning (including goal setting and scenario analysis)
    - Operational decision making (including financial planning and supplier vetting)
    - The organization's risk management framework (including the enterprise risk register and business continuity planning).

## Heads of ERM: Assess and Escalate Risks While Supporting Risk Owners

**Analysis by:** Ben Fisher, Steve Shapiro

Heads of ERM must help their organizations navigate a range of new and intensified threats related to the war. While heads of ERM may contribute to immediate crisis management activities, it should not come at the expense of the forward-looking work required to prepare the organization for knock-on disruptions and longer-term fallout.

Prioritize the following actions:

- **Assess shifts in organizational risk exposure.** Evaluate how the war alters exposure across critical risk categories like supply chain, people, cybersecurity, operations and financial stability. Identify where vulnerabilities are increasing.

- **Develop and stress-test scenarios.** Consider multiple ways the war could evolve to determine the most disruptive or least desirable future states. Map the consequences the organization would face if these scenarios materialize.

- **Escalate priority risks for immediate action.** Surface a focused set of high-impact risks to the board or executive risk committee, and recommend near-term response actions.

- **Support owners of new or amplified risks.** Direct your support to where execution is likely to break down. Connect risk owners to the right expertise and practical tools. Focus on detecting and correcting harmful inconsistencies and ensuring cross-functional alignment, while allowing flexibility where it is justified. Use your time in incident response and business continuity management (BCM) committees to spot early signs of misalignment.

## Chief Procurement Officers: Expect Disruption Even Without Direct Buying From Iran

**Analysis by:** Michael Ryan, Cheryl Van Dyke

While the U.S. and EU strictly limit direct business with Iran, the current war will present indirect global impacts through Iran's major importers in South and Southeast Asia, as well as overall global market reactions. As a result, CPOs must not dismiss the Iran war as unrelated to their organization's global procurement activities, even if they don't see direct procurement links.

Indirect impacts may not be evident immediately, so CPOs have a small window to proactively initiate the following actions:

- **Assess the vulnerability of critical spend categories and associated supply bases.** Review your product and service lines, aligning them with categories of spend to identify weaknesses. Pay close attention to critical spend categories with deep roots or strong dependencies in the Middle East, such as oil and gas, petrochemicals, chemicals, plastics, metals, minerals, and agricultural products.

- **Engage with suppliers to gain transparency on upstream risks.** Hold information sessions with your suppliers to clearly articulate the implications of current events. Ask suppliers to not only identify any known impacts, potential risks and proactive management plans for their environment, but also cascade that down to their suppliers for multitiered visibility.

- **Review, update and iterate to support longer-term strategies.** Identify the sources and intelligence that will trigger future action as the situation continues to evolve. You and your teams must understand and align stakeholders to the enterprisewide risk appetite. Then, create category-specific scenario plans and drills focused on the near- and midterm to help mitigate impacts.

## Heads of IT SPVM: Prioritize Dynamic Resilience Over Cost Optimization

**Analysis by:** Danny Kreidy, Aadil Nanji

Heads of IT sourcing, procurement and vendor management (SPVM) must pivot from cost optimization to dynamic resilience. It is critical to secure the digital supply chain against logistics paralysis, cyberthreats and regulatory shifts.

Prioritize the following actions:

- **Establish a "war-sourcing cell."** Set up a cross-functional team (including sourcing, security, legal and finance) with delegated authority to map vendor exposure daily and drive rapid decisions.

- **Implement an "order freeze exception" gate.** Control buying by instituting a 10- to 15-minute triage gate for critical orders. Prioritize security items (e.g., firewalls, MFA tokens), network/data center spares and components heavily dependent on disrupted air-freight corridors.

- **Execute targeted inventory buffering.** Avoid blind hoarding; instead, secure 30 to 60 days of spares for critical operational and recovery inventory. Focus strictly on items with a single OEM, a single logistics lane or a single on-site engineer dependency.

- **Conduct a vendor exposure sweep.** Assess Tier 1 vendors within 48 to 72 hours. Demand evidence of their geographic delivery chains, logistics contingency plans and remote delivery readiness.

## Chief Marketing Officers: Safeguard Brand and Budget

**Analysis by:** Ewan McIntyre

During major global crises, marketing may seem to experience no immediate impact. However, inaction is not an option. Chief marketing officers must take decisive steps to ensure their teams are prepared, their brands are protected and their organizations remain agile as the situation evolves.

Prioritize the following actions:

- **Coordinate with your communications team.** Share information and coordinate messages so your brand speaks with one clear, timely voice. Stay alert to fast-changing news, and be ready to adjust your messaging as needed.

- **Review all current media activity.** Direct your teams and agencies to assess campaigns, placements and automated content for potential risks or sensitivities in the current climate. Empower them to pause or adjust activity as needed to protect brand safety.

- **Plan for budget challenges.** Assemble your leadership team to map out best, worst and likely scenarios. Prioritize essential marketing activities, and identify where you can flex or cut spending if needed.

## Contributors

Chris Audet, Matt Hoyles, Peter Young

## Evidence

[1] Iran Escalates Retaliatory Strikes as U.S. Signals Long Battle, Live Updates, The New York Times.

## Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

First Take: Iran Conflict Demands Immediate Executive Action, Even If You're Outside the Middle East

The 2026 Iran Conflict Forces IT Sourcing to Prioritize Resilience Over Cost

# Connect with us

Get actionable, objective business and technology insights that drive smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

**U.S.:** 1 855 322 5484

**International:** +44 (0) 3300 296 946

Become a Client

**Stay connected to the latest insights**

**Attend a Gartner conference**

View Conferences

Gartner®