What To Do When Your Executive or Company Takes a Public Stance — or Chooses Silence

Executives and organizations are under growing pressure to comment on social and political issues. In fact, a 2025 Gallup study found that 51% of U.S. adults believe companies should take a public stance on current issues.

Whether an executive speaks out, remains silent, or a company takes a visible stance, the organization's risk profile can shift instantly. What's more, executives aren't always trained to carefully walk a line to keep everyone happy. They typically speak candidly. Even with strong PR support, navigating these moments can be complex, and well-intentioned decisions can carry unintended consequences.

Security's role isn't to shape the message. It's to anticipate the impact, reduce exposure, and prepare the organization to respond. This checklist outlines how your team can prepare and get ahead of threats using the following framework:

Align → Detect → Mitigate → Respond

1. Align: Establish early internal alignment

This represents the ideal state. Many teams may not yet have the internal alignment needed to ensure timely information sharing ahead of a decision to speak out or stay silent. That said, building these relationships in advance is critical, and they're far easier to establish before an issue escalates than in the middle of one.

Build and maintain trusted relationships with: • Executive Assistants • Corporate Communications, PR, or Marketing • Legal • HR	☐
Educate partners on why security needs early visibility to manage exposure and response, not block decisions. Emphasize the need for advance notice of: • Issues under consideration • Drafting timelines for statements • Decisions to not make a statement • Major cultural or brand decisions (like DEI changes, Pride Month participation)	☐
When meeting with cross-functional teams, take note of the following: • What's being said and when it may become public • Who will be associated with the decision (company vs. named executive)	☐

2. Detect: Research and monitor

Whether you're preparing for a statement or responding to one already made, the first step is to research and monitor relevant sentiment and key actors.

Conduct baseline research on: • The issue itself • Relevant activist or advocacy groups • Known individuals with a history of escalation	☐
Establish monitoring for: • External sentiment online (positive and negative) • Internal sentiment among your workforce — via approved channels and in partnership with HR and legal	☐
Watch for key signals like: • Changes in the "daily rhythm" and tone of conversation • Early rumblings that precede public escalation • Mentions of executive names, family members, home locations, or travel	☐
Centralize and track information about: • Threat actors • Escalating narratives • Credible threats	☐
Audit the executive's digital footprint, including: • Social media presence (active and historical) • Public affiliations or past statements that could be resurfaced • Personal information that could be weaponized	☐
Monitor online chatter for: • Mentions of family members • Attempts to connect them to the issue • Doxxing indicators or crowd-sourced research	☐
Extend your review to immediate family members and known associates who may be publicly visible	☐

If your team lacks dedicated EP analysts, proactively source this intelligence rather than assuming it doesn't exist.

Tools like Ontic help ensure this intelligence isn't siloed.

3. Mitigate: Timing, travel, and exposure coordination

Based on the information you've gathered, adjust posture where needed to minimize risk without defaulting to executive travel or movement cancellation.

If given advanced notice, align with Comms/Marketing on: • Timing of announcements or statements • Channels that will be used for the statement • Likely follow-on coverage or amplification	☐
Proactively evaluate executive exposure: • Upcoming travel, events, or appearances • Public-facing moments tied to the issue • Predictable routines or patterns	☐

Security's role is to enable business as usual, not bring it to a halt.

Continued on next page

Make low-friction adjustments where appropriate: • Modify timing, routes, or visibility • Shift formats (virtual vs. in-person) • Quietly reduce exposure without signaling alarm	☐
Clearly communicate posture adjustments to: • Executives • EAs • Relevant internal teams	☐
Tie mitigation decisions to observable intelligence to avoid ambiguity or overreaction.	☐

4. Respond: Prepare for escalation

Ensure your response muscle is ready before it's needed.

Revisit and validate response protocols for: • Credible threats to executives • Online-to-offline escalation • Protest or disruption activity • In-person targeting	☐
Confirm escalation criteria and thresholds: • What elevates a concern to a credible threat • When monitoring transitions to active response • When external partners or law enforcement are engaged	☐
Clarify roles and decision ownership: • Who receives time-sensitive intelligence • Who has authority to approve response actions • Who coordinates execution across teams	☐
Pressure-test readiness: • Are protocols current and actionable? • Are contact lists up to date? • Are decision-makers reachable outside normal hours?	☐
Ensure documentation and reference materials are accessible: • Response playbooks • Escalation trees • Emergency contacts	☐