

Q3 2025

Top Risk: Trump's Tactics Taking a Toll



Global Risk Advisory Council

Message From The Chair

Over the past several years—as an entrepreneur, while leading the U.S. Small Business Administration, and now through my work on the Global Risk Advisory Council's Reputation Risk Index—I have watched closely as organizations face a hyper-polarized, technology-amplified risk landscape. This quarter's results signal a tipping point. While brand strength had not been overly impacted by government cuts, tariffs, and political discourse, we are now seeing the landscape shift over this past summer.

The most striking development is how President Trump's ability to use his platform and policy levers to target individual executives and companies has transformed political rhetoric into a distinct reputational risk category. We have seen again and again how criticism from the current administration poses a major reputational threat, particularly as it mobilizes the President's base against companies like Cracker Barrel or Microsoft. Lone actors, amplified by MAGA influencer accounts and adopted by the President, can now trigger risks that exacerbate conventional corporate vulnerabilities—a single social media post, at times AI-generated, can spark a crisis. The bipartisan Global Risk Advisory Council identified "Targeting by or criticism from Donald Trump" as the #1 reputational risk in Q3 2025, with one Council member stating that compared to the other nine risk categories, "it's not even close: the 'criticism from Donald Trump' is unfortunately a 100 not a 10."

Organizations also face unprecedented complexity on other reputational risk fronts, according to the Q3 report: fraud accusations and ethics failures are magnified and amplified under unprecedented and intense public scrutiny, while perceived anticompetitive practices are drawing renewed attention from enforcement bodies. Also notable is that digital and AI platforms are amplifying allegations on all risks on a large scale. Without proper guardrails, public trust in a company can collapse quickly in this environment.

The Council's analysis revealed a business environment shaped by what Global Situation Room has labeled "amplified accountability convergence"—where AI capabilities, political polarization, and the unprecedented reach of influencers now magnify traditional reputational risks. And while technological advancements offer powerful tools that can buttress businesses, they also come with unprecedented risks. AI creates new opportunities, but challenges as well with the spread of false information, lack of human oversight, mental health harm, IP infringement, and discrimination. Together, we are navigating a new technological landscape, and with these new opportunities, we must recognize the potential reputational pitfalls.

As we track and share these shifts in our quarterly index, I urge leaders to consider reputational risk management as essential business infrastructure—not an optional safeguard. The companies that give due focus on the convergence of AI, political polarization, and individual influence will endure and thrive. Those who don't will find themselves overwhelmed.



Isabel Casillas Guzman
Global Risk Advisory Council Chair
Avenida Advisors Founder and President

Top Risk

The Council identified public criticism from Donald Trump as the leading reputational risk in the third quarter. Targeting by the President, his administration, and allies has garnered widespread attention in the media and online communities, culminating in significant revenue and reputational consequences. Even companies that don't seek to draw the ire of the administration can find themselves on the wrong side of its policies can face massive reputational damage. Take, for instance, Trump's "woke AI" executive order. It instructs companies to address alleged bias in AI systems and failure to comply can put federal contracts at risk. Critics argue this creates perverse incentives that can weaken AI safety protections. Another example is when Trump imposed a \$100,000 fee on new H-1B visas. Major tech companies—Amazon, Microsoft, Meta, Apple, and Google—scrambled to maintain favor with the administration, desperate to avoid losing access to the foreign talent pipeline that powers their operations. Whether through executive orders that reshape industry practices or visa fees that threaten talent pipelines, businesses that cross Trump face substantial risk: his social media reach and Republican control of Congress give him unprecedented power to back up his threats with Congressional action, adding to the reputational and revenue damage.

The Global Risk Advisory Council

Members of the Global Risk Advisory Council have shaped crisis response in the Situation Room and steered strategy in boardrooms worldwide. The Council's 130+ members include former heads of state, government ministers, and senior public affairs executives—all of whom are invited based on their proven influence at the highest levels of public debate. They bring expertise spanning sectors, continents, and domains of power.

Global Risk Advisory Council By The Numbers



20+ Countries

5 Continents
Represented



15

Former Heads of
State and Ministers



130+
Members



15
CEOs



16

Global Fortune
500 Companies
Represented

Meet Some of Our Members



Karen Sommer Shalett
Director of External Communications,
Templeton World Charity Foundation



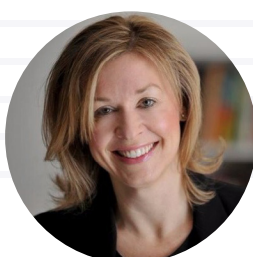
Alexandra Pasternak-Jackson
CEO,
Amcham Finland



Michael D'Arcy
*Former Irish Minister of State at the Department
of Finance for the Leo Varadkar Administration*



Eugene Laney
President and CEO,
American Association
of Exporters and Importers



Mary Whenman
Managing Director,
Communications and Marketing,
British Business Bank



Aliza Bran
Director of Media Relations,
Spy Museum



Thórdís Kolbrún R. Gylfadótti
Former Foreign Affairs Minister of Iceland



Rochelle Ford
CEO,
Arthur W. Page Society



Paul O'Brien
Head of Public Affairs,
Bank of Ireland Group



Tim Cummins
President,
World Commerce And
Contracting Association



Peter Selfridge
*Former Global Head of
Government Affairs, SAP*



Ty McKeiver
*Former Director of Public Affairs,
International Trade Administration*

Q3 Spotlight on Tech: Top Reputation Risks Ranked

#1

Targeting by or criticism from Donald Trump

Donald Trump publicly attacking or criticizing an executive or organization.

#2

Fraud

Perceived deception used to gain money or personal advantage, often involving lies or false documents.

#3

Organizational ethics failures

When a company is accused of violating ethical standards.

#4

Data privacy violations

Violations of consumers' right to control how their personal data is collected, used, or shared.

#5

CEO controversy

Scrutiny or public criticism of a CEO's behavior, decisions, or potential departure that could undermine investor or public confidence.

#6

Discrimination

Alleged unfair treatment of individuals or groups based on race or another protected status, often in areas like employment, housing, or education.

#7

IP/copyright/trademark infringement

Claims of copying creative works, inventions, or ownership, including unauthorized use, reproduction, or distribution of copyrighted, patented, or trademarked material.

#8

Executive leadership (non-CEO) controversy

Negative attention surrounding a company's leadership team due to misconduct, poor decision-making, or damaging public statements or rumors.

#9

Anticompetitiveness/antitrust

Business or government actions that are seen to restrict competition, leading to higher prices, lower quality, reduced service levels, or less innovation. Includes unfair market practices, monopolistic behavior, and legislation aimed at preventing or regulating trusts and monopolies to ensure fair competition.

#10

Elon Musk association/criticism

Instances where an individual, company, or entity is associated with, targeted by, or publicly criticized by Elon Musk.

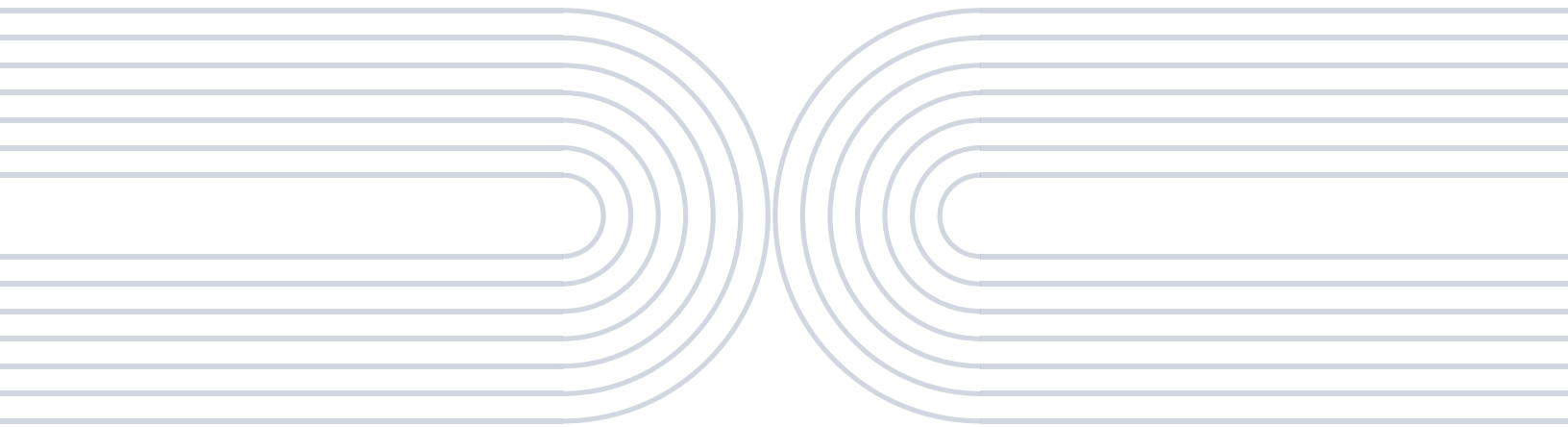
Comparing Q2 and Q3 Rankings

Risk	Q3 Ranking Technology Focused	Q2 Ranking Europe Focused	Difference
Anticompetitiveness/ Antitrust	9	9	=
CEO controversy	5	6	↑+1
China ties	Not ranked	7	—
Climate change/ environmental harms	Not ranked	8	—
Corruption	Not ranked	3	—
Data privacy violations	4	2	↓-2
Disinformation	Not ranked	1	—
Donald Trump	1	Not ranked	+
Elon Musk	10	Not ranked	+
Executive Leadership Controversy	8	Not ranked	+
Fraud	2	Not ranked	+
IP/copyright infringement	7	10	↑+3
Major operational disruptions	Not ranked	5	—
Organizational ethics failures	3	4	↑+1
Discrimination	6	Not ranked	+

Charting Our Course Through Q3

In Q3, we focus on the space experiencing the most volatile reputational landscape: the technology sector. With AI as the catalyst, tech companies now face unprecedented challenges that are dominating headlines, social media chatter and reshaping the landscape of corporate reputation at breakneck speed.

Artificial intelligence has transformed reputation management from one involving a narrower array of public relations tactics into a broad fight for truth and survival. Companies face manufactured content in a rapidly shifting technology and media environment. One Council member described the threat landscape as defined by, "deep fakes that magnify weaponized information." Fake content is now so convincing that it can damage a company's reputation before it is detected. Beyond AI-specific threats, companies face scrutiny across the entire digital ecosystem, including data privacy breaches that expose millions of user records, algorithmic bias in hiring platforms that trigger discrimination lawsuits, and cybersecurity vulnerabilities in cloud infrastructure that compromise client data. The stakes are higher because "public trust in science and research has been disastrously eroded"—facts no longer guarantee a favorable perception.



Companies face backlash for adopting AI too slowly and for mismanaging it when they do—chatbots producing biased outputs, autonomous vehicles causing accidents, facial recognition systems misidentifying individuals, and algorithms promoting harmful content without oversight. This unfolds in a largely unregulated space where policy shifts constantly: cryptocurrency regulations, semiconductor export controls, social media content moderation requirements, and antitrust investigations. Companies must address immediate threats while preparing for the potential breakthroughs of quantum computing and addressing concerns related to augmented reality privacy.

Prominent companies have aligned themselves with the current administration to navigate the shifting technology sector, AI challenges, and policy upheaval. Chipmaker NVIDIA and social media platform TikTok exemplify this strategy. NVIDIA navigated semiconductor export restrictions by creating China-compliant chip technology, positioning itself as a cooperative partner in U.S. technological sovereignty rather than fighting the restrictions. TikTok distanced itself from its Chinese parent company, ByteDance, by partnering with American companies for data hosting, relocating content moderation operations to the United States, and committing to transparency measures that address national security concerns. Both companies worked to reduce the reputational risk associated with their work in China by tightening ties to the Trump administration. Both proactively addressed the administration's concerns about Chinese technological influence while demonstrating tangible value to U.S. strategic interests.



#1 Top Risk: Targeting By or Criticism From Donald Trump

Political targeting by President Trump in the press, along with social media, and the federal government action that generally follows now ranks as the most dangerous business risk. The threat from presidential targeting has intensified over the last quarter, creating a chilling effect across corporate America. Companies in his crosshairs are facing consumer boycotts, investor flight, and stock devaluation. The damage can escalate to regulatory retaliation, terminated government contracts, and federal agency scrutiny that imposes extreme compliance costs and operational disruptions.

“ There is more of a reputational risk by capitulating to Trump's demands than being targeted by him.”

—Council Member

“ ABC/Disney is the latest to capitulate to the administration based on the jokes of a comedian, late-night talk show host. Compared to the other nine categories, it's not even close: the 'criticism from Donald Trump' is unfortunately a 100, not a 10.”

—Council Member

CASE STUDY: Intel CEO and Trump: From Conflict to Partnership

In August 2025, Trump publicly demanded the resignation of Intel CEO Lip-Bu Tan, calling him "highly CONFLICTED" over past investments in Chinese semiconductor firms. Arkansas Senator Tom Cotton had flagged security concerns about Tan's Chinese ties and his previous role at Cadence Design Systems, which violated export controls by selling to Chinese military universities. Intel's stock dropped.

Within four days, Tan met Trump at the White House and reversed the crisis. Intel agreed to give the U.S. government a 10% stake worth \$8.9 billion—a deal Trump hailed as "great for America." The turnaround proved that swift alignment with presidential priorities, backed by concrete concessions, can neutralize even the most public attacks. Yet, such a direct interventionist approach in private companies has left many observers worried of what it portends for the future of American capitalism.

#2 Top Risk: Fraud

In the current economic climate, accusations of fraud can carry exceptionally high costs. Even if companies are ultimately vindicated or the truth ends up being less serious than initially thought, the short news and social media cycles have long since left it behind. This makes it extraordinarily difficult to recover. Social media realities create conducive conditions that allow fraud allegations to proliferate rapidly. With influential individuals commanding siloed media ecosystems, fraud allegations spread virally—regardless of merit. Routine regulatory probes escalate into scandals as influencer networks outpace corporate fact-checking. As one Council member notes, modern fraud accusations operate "at the intersection of legitimate enforcement and competitive warfare," blurring the line between whistleblowing and strategic attacks.

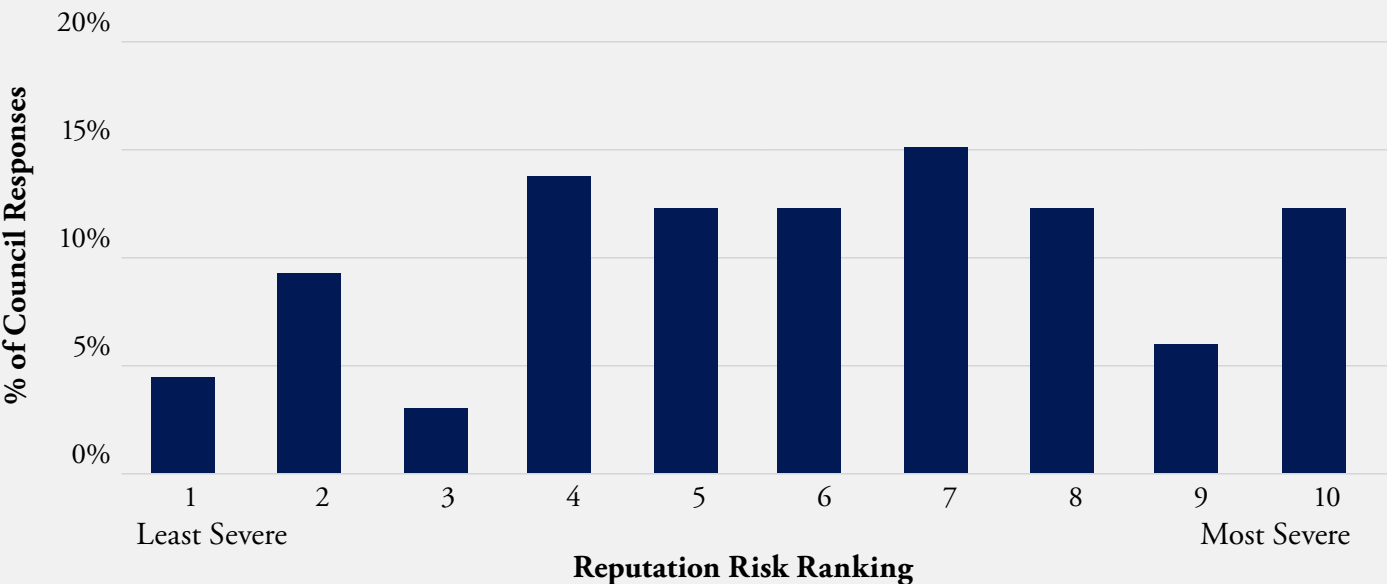
As another Council member warns, "As the economy and businesses struggle over the next 8 months, look for an increase in fraud accusations targeting companies." Business leaders increasingly face a dual threat: actual fraud prosecutions and weaponized fraud allegations from competitors and amplified on social media. The challenge extends beyond traditional compliance to defending against coordinated campaigns that can manufacture the appearance of fraudulent behavior through the manipulation of evidence or the selective presentation of legitimate business practices. In Q3, more than 60% of Council members surveyed rated fraud allegations an '8' or greater in severity, reflecting both the legal consequences and reputational damage that can result from accusations alone.

For leaders navigating this environment, traditional fraud prevention is no longer sufficient. Success requires comprehensive monitoring systems that track not just compliance metrics but also social media sentiment, influencer activity, and coordinated campaign patterns.

“Grassroots social media influencers are a very significant danger and can be stoked by hidden actors/astroturfing experts.”

–Kevin Kent, Transatlantic Practice Chair, Clark Hill

How the Council Ranked Fraud



CASE STUDY: DOJ Investigation of United Healthcare

The Department of Justice's investigation into United Healthcare began quietly in 2024. Still, it escalated dramatically throughout 2025, representing one of the most significant healthcare fraud probes targeting the nation's largest private health insurer. The Wall Street Journal first reported about the investigation in February 2025, revealing that federal investigators were examining UnitedHealth's Medicare billing practices, including potential overpayments in its Medicare Advantage program and at physician practices the insurer owns. Initially, UnitedHealth denied being notified and called the reporting "deeply irresponsible," but by July 2025, the company formally acknowledged the investigation in a securities filing, stating it had proactively reached out to the DOJ and begun complying with formal criminal and civil requests.

The investigation has had major financial and brand consequences for UnitedHealth, with the company's stock losing approximately half its value over the past year, representing a market capitalization loss of more than \$277 billion. The crisis coincided with significant leadership upheaval, including the surprise departure of CEO Andrew Witty in May 2025 and the company's suspension of its 2025 financial guidance due to higher-than-expected medical costs. This took place despite the company's claims of, "full confidence in its practices" and citing independent CMS audits confirming its practices are, "among the most accurate in the industry."

#3 Top Risk: Organizational Ethics Failures

Organizational ethics failures have consistently drawn scrutiny and controversy. In September, OpenAI faced renewed ethical questions when former safety researchers alleged the company had prioritized rapid product deployment over comprehensive safety testing. The controversy included claims that safety protocols were bypassed and that researchers who raised concerns faced internal pressure to remain silent. While OpenAI has disputed these characterizations, the incident has highlighted the tension between the speed of innovation and ethical responsibility that AI companies face.

One Council member warns that the current reduction in enforcement in the United States may be creating a false sense of confidence among corporate leaders. They note that, "Risks associated with organizational ethics have heightened under the current administration, given the perception supported by formal government statements that enforcement priorities are elsewhere. When a business faces mounting competitive challenges, individuals often make risk-based judgment calls. While the current enforcement policy may be focused on other issues, that can and will change within the window of potential liability for those decisions that prove wrong in hindsight." Yet, this belief may be shortsighted and overlooks the broader regulatory environment. Enforcement varies significantly across jurisdictions and sectors. European markets demonstrate particular sensitivity to ethics failures, where data privacy violations lead to immediate reputational and legal consequences.

Such ethical accusations do not always leave a permanent scar. Indeed, they can be powerful moments for elevating and enhancing a company's reputation. Council member Fanella Grey notes that reputational risk drops when handled well, suggesting that a transparent and rapid response can mitigate long-term damage when organizations acknowledge and address ethical failures promptly.

“Combating disinformation spread by executive leaders both in government and corporate is a full-time job on top of a full-time job.”

—Elizabeth Rosenberg, Founder, The Good Advice Company

How the Council Ranked Organizational Ethics Failures



CASE STUDY: State Farm California Wildfire Investigation

In June 2025, California Insurance Commissioner Ricardo Lara launched a formal investigation into State Farm's handling of wildfire claims from the January 2025 Los Angeles fires. The Palisades and Eaton wildfires destroyed over 16,000 buildings and killed 30 people, generating thousands of insurance claims. State Farm received 12,855 fire-related claims and paid over \$3.96 billion by June 2025.

The investigation focused on several key problems: fire survivors being assigned multiple adjusters with poor communication, inconsistent handling of similar claims, and inadequate record-keeping. Customers reported fighting for smoke damage reimbursements and experiencing significant payment delays. In one notable case, a fire survivor's \$876,354 State Farm check was placed on hold due to insufficient funds. The state insurance department has already recovered over \$40 million for wildfire survivors through intervention, highlighting the scope of the issues. This investigation will determine whether State Farm violated California's consumer protection laws while handling claims from one of the costliest natural disasters in U.S. history.

Understanding the AI and Tech Divide in Reputational Risk

In the past, technological reputational risks were mainly operational, encompassing system failures, data breaches, and software bugs. These risks were inherent. However, they have now transformed into existential threats, influenced by artificial intelligence, deregulation, and the rapid scalability of these dangers.

In response to our Q3 survey, members of our Global Risk Advisory Council highlighted that AI-driven risks are fundamentally different from traditional technology threats. As one Council member observed, "A major risk lies in being unable to counter AI-generated attacks, especially when they are globally coordinated and designed to cause maximum harm in a short time. Such incidents can inflict lasting harm on vital relationships and erode trust among key audiences at critical moments."



While AI offers organizations powerful tools for efficiency, it also creates unprecedented risks, giving critics new ways to damage reputations quickly and at scale. Although many organizations are investing in defenses against AI-driven attacks, the pace of technological change will make it difficult for them to keep up."

—Council Member

One very important aspect affecting the prevalence and speed of such threats is the ever-changing regulation (and by that same merit) deregulation landscape. Council members report that the removal of content moderation standards and oversight mechanisms creates what one described as a "super-spreader environment" for reputational threats. In this landscape, the traditional boundaries between digital reputation management and physical safety have collapsed entirely.

The stakes transcend individual companies—institutional trust itself is at risk. AI-generated disinformation at scale, combined with platforms stripped of guardrails, fractures our shared reality. As one Council member put it: "The greatest reputational risk to companies is the lowering of the standards of what is considered truth."

Top Reputation Risks Stemming From AI Misuse

Ranked by Media Coverage



#1

Spread of false information



#2

Lack of human oversight



#3

Mental health harm



#4

IP infringement



#5

Discrimination

What Council Members Are Saying

“

When a reputational risk becomes a physical risk, the game completely changes. The potential damage for any company associated—even indirectly—with that violence is magnified exponentially. It's no longer about managing a narrative; it's about being linked to tangible harm and human tragedy, a stain that's nearly impossible to remove."

—Cate Costa, Principal, GSImpact

“

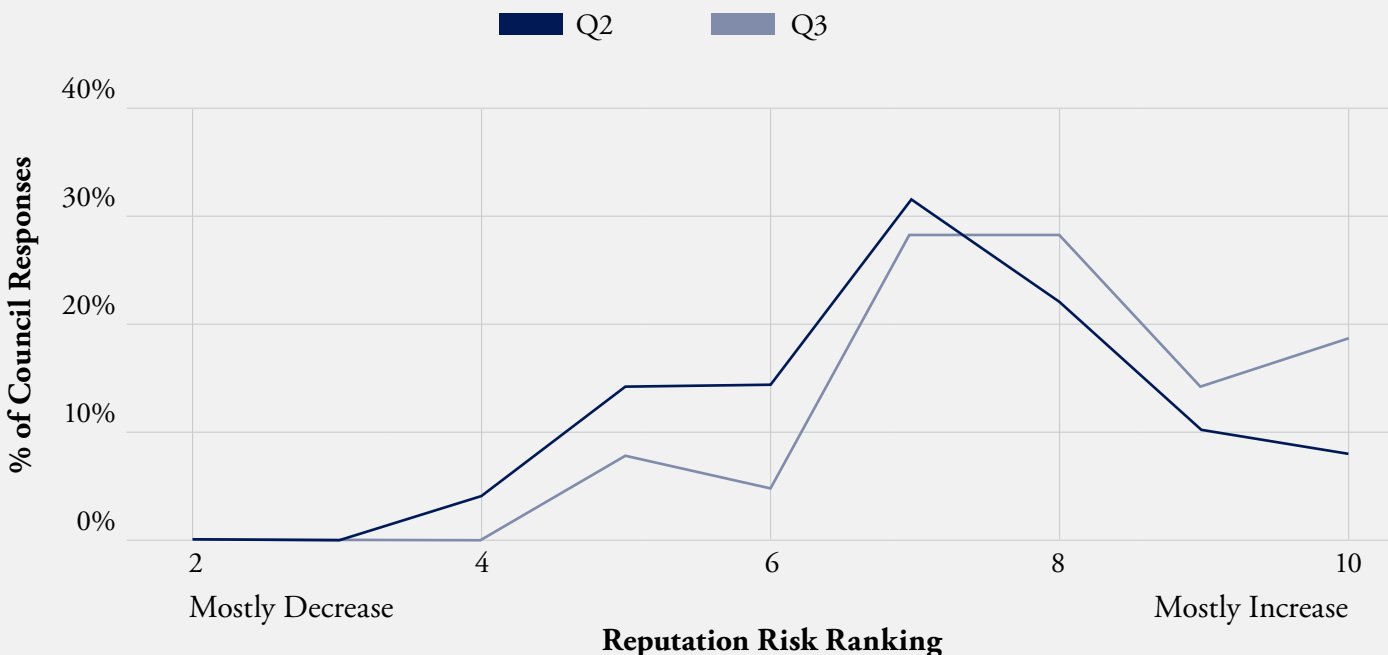
A worsening bot-to-human ratio online coupled with lower content moderation standards leads to a deeply unpredictable information environment - hard for companies to navigate business-wise or to predict how their image might fare in a given scenario."

—Kellee Wicker, Vice President, Technology, Innovation and Space, Meridian International Center

Reputational Risks Leaders Are Watching Closely

Council members have forecast that Reputational Risks will increase on some level each quarter during this year, with a majority rating an increase of '7' or '8' on a scale of 1, indicating a significant decrease, and 10, indicating a substantial increase.

How much do you think reputational risks will increase or decrease in severity over the next 3 months?



Public affairs leaders are broadening their lens to monitor reputational risks beyond their traditional remit. When asked about risks they're watching closely, Council members cited the confluence of political volatility and tech, creating severe problems with violence, such as the assassination of UnitedHealthcare CEO Brian Thompson. Other Council members are concerned about underage users turning to AI in dangerous ways, such as the suicide case involving Character.AI.

Here's what members of the Council will be watching closely moving forward:

- U.S. Political Volatility
- AI Misuse
- Spread of Misinformation
- Decline of Youth Mental Health
- Tariffs
- Data Privacy
- Association with Drug Cartels
- Political Violence
- Distrust in Government

"The aftermath of the assassination of Charlie Kirk has left us in uncharted waters as the government plans a coordinated attack on nonprofits in violation of freedom of political speech protections."

—Council Member



The current political environment has made discriminatory language and practices more mainstream, but this environment is temporary. History gives us a stark warning: after World War II, those who aligned themselves with antisemitic and racist ideologies could not escape the reputational fallout, even if their positions felt safe during the conflict."

—Cate Costa, Principal, GSImpact





Global Situation Room, Inc.

Complex Communications®

www.ReputationRisk.org

