

Q1 2026

Focus on Philanthropy



Global Risk Advisory Council

Introduction

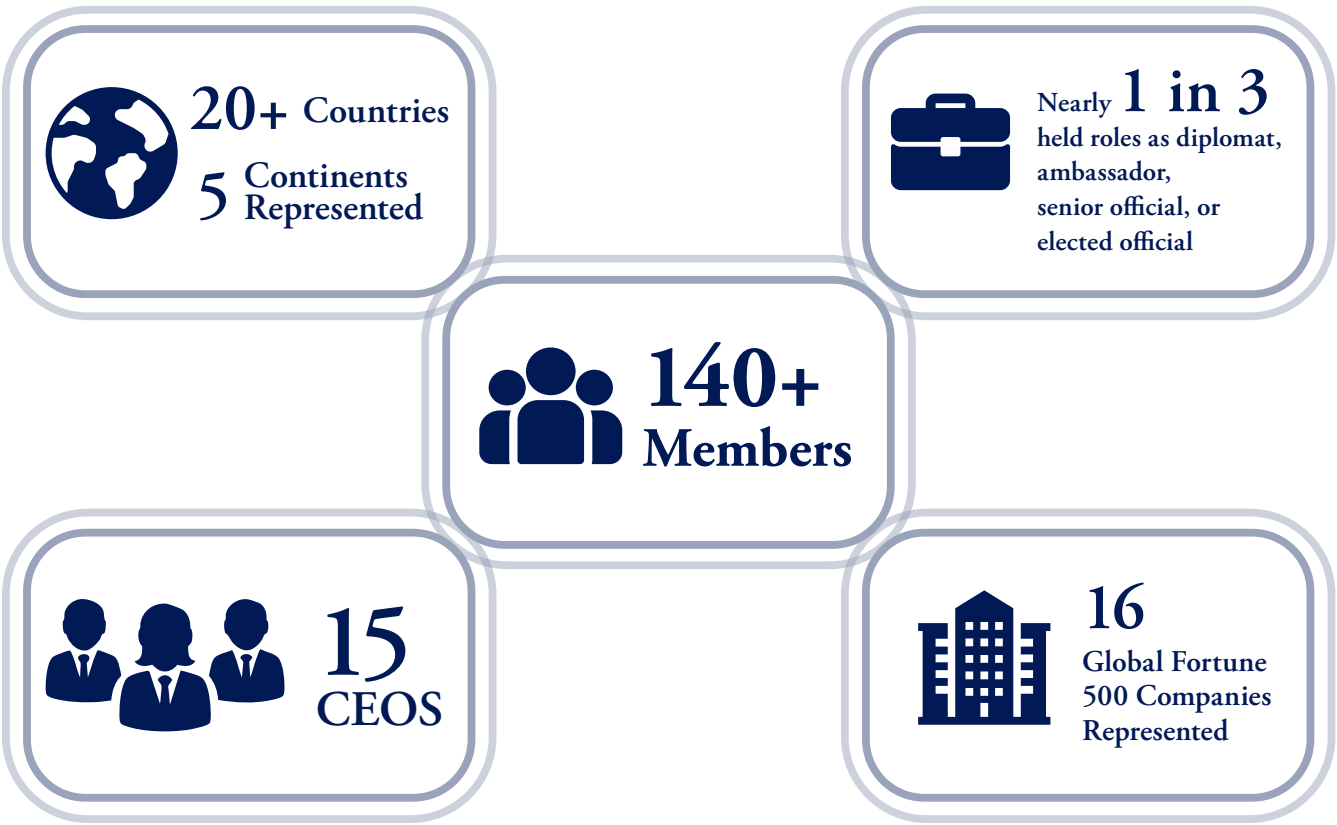
The Q1 2026 Reputation Risk Index marks a turning point, with traditional paradigms for protecting a company’s brand overturned; the old rules no longer seem to apply. We’ve entered an era where maturing AI and extreme political volatility have collided, making traditional risk management feel dangerously outdated. This isn’t a slow evolution—AI has officially shifted from a technical concern to a primary driver of legal and financial instability.

This quarter, we are focusing on the philanthropic sector, which is currently stuck in a "politicization trap." Foundations are being targeted for their core missions—such as climate change and immigration—while also being flooded with "AI slop" applications that threaten to overwhelm traditional grantmaking. This report highlights the threats all organizations must confront in 2026 and, separately, serves as a report card for the philanthropic sector.

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 140+ 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



Meet Some of Our Members



Rochelle Ford
CEO, Arthur W. Page Society



Robert Bole
Head of Innovation and
Strategy, Signal



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



Christopher Smart
Managing Partner, Arbroath Group



Bridgette Stumpf
CEO & Co-Founder, Volare



Antwaun Griffin
General Manager, Socially Responsible
Purchasing, Amazon Business



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



Stephanie Agee
Senior Vice President and Chief
Administrative Officer, International
Trade, Virginia Economic
Development Partnership



Todd Haymore
Managing Director, Global
Economic Development, Commerce
& Government Relations, Hunton
Andrews Kurth LLP



Fenella Grey
Co-Founder, Hello Tomorrow



Jed Willard
Executive Director, FDR Global
Engagement Initiative



Elizabeth Rosenberg
Founder, The Good Advice Company

Message From The Chair

As we move further into 2026, the unprecedented transformation fueled by rapid tech advancement and political volatility that we tracked throughout last year has shifted from a looming threat to a permanent operational reality. The rapid maturation of artificial intelligence and its deepening integration into our global economy isn't just a trend anymore—it is the foundation of the modern risk landscape across multiple dimensions.

In the first quarter – and for the first time – AI misuse has solidified its position as the primary reputational threat for half a year running. What was once a concern about isolated deepfakes, misinformation and humans replaced with unhelpful chatbots, has evolved into a systemic enabler of reputational, legal, and financial chaos. While companies move quickly to become agentic enterprises and realize the positive gains of AI to advance growth and greater efficiency, tensions persist with negative economic concerns over workforce, intellectual property, and overall safety. To add further complexity, “data breach” has hit the risk index for the first time landing in the top three – furthering risk as companies drive data expansion to create stronger use cases for AI and automation.

Against this volatile backdrop, we are focusing the Q1 2026 Index on the Philanthropic Sector—an industry still distraught by volatile politicization fueled by our second ranked risk: “targeting by or criticism from Donald Trump.” Foundations are finding their core missions, from climate change to DEI programs, weaponized against them – and all at a time when federal funding for social safety net programs is being cut and AI advances.

These pressures are further complicated by a global environment on edge. The stakes have moved beyond simple communication strategies. In order for organizations to fortify against reputational risks in 2026, they must bridge the gap between their stated values and the realities of operating in an highly politicized, AI-driven world. The prediction from our Council is unanimous: these risks will only sharpen as the year progresses. Resilience now depends on a bone-deep understanding of how technology, politics, and shifting social influences collide to redefine our global economy.



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

Q1 Top Reputation Risks Ranked

#1

AI misuse

Harmful or deceptive use of artificial intelligence, including deepfakes, misinformation, biased decision-making, or other unethical applications that cause harm or manipulate public perception.

#2

Targeting by or criticism from Trump

Negative attention or consequences resulting from criticizing Donald Trump or when Donald Trump publicly attacks or criticizes an individual or organization.

#3

Data breach

Unauthorized access, exposure, or theft of sensitive or personal information, often due to poor security.

#4

Major operational disruption

Events like natural disasters (e.g., wildfires, pandemics) or artificial crises (e.g., shootings, explosions)

#5

Child safety/harm

Actions or accusations of putting children at risk of mental, emotional, or physical harm.

#6

Deceptive marketing

Misleading ads or sales tactics used to trick people into buying something or believing false claims.

#7

Breach of contract

When one party fails to meet the agreed terms of a legal settlement or violates specified terms, resulting in potential legal or financial consequences for the affected parties.

#8

Anticompetitiveness / antitrust

Business or government actions that 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.

#9

IP/copyright/trademark infringement

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

#10

Elon Musk

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

Comparing 2025 Q4 and 2026 Q1 Rankings

Risk	2026 Q1 Ranking	2025 Q4 Ranking	Difference
AI misuse	1	1	=
Anticompetitiveness/ Antitrust	8	5	↓-3
Breach of contract	7	Not ranked	+
Child safety/harm	5	4	↓-1
Consumer protection	Not ranked	7	-
Data breach	3	Not ranked	+
Data privacy violations	Not ranked	3	-
Deceptive marketing	6	Not ranked	+
Donald Trump	2	2	=
Elon Musk	10	Not ranked	+
Fraud	Not ranked	6	-
IP/copyright infringement	9	9	=
Major operational disruption	4	Not ranked	+
Securities fraud	Not ranked	8	-
Securities violations	Not ranked	10	-

#1 Top Risk: AI Misuse

In the first quarter of 2026, AI misuse emerged as the preeminent reputational threat, with 53% of Council members ranking it '8' or higher. AI is no longer viewed as a standalone technical glitch but as a "systemic enabler" that heightens every other risk category. As regulation continues to trail behind the technology's rapid maturation, harmful applications—such as biased decision-making and AI-generated misinformation—have become pervasive, integrated into the very fabric of corporate and political interaction.

The consensus among Council experts is that AI acts as a force multiplier for existing crises rather than just creating new ones. By automating the production of deepfakes and streamlining the violation of intellectual property, AI allows reputational damage to occur at a scale and speed that traditional crisis management is ill-equipped to handle.

“ Trump’s threats and AI misuse continue to be a major source of risk to reputation, and show no signs of letting up anytime soon.”

—Lee Poston, Principal, Saola Strategies

The tension between technological capability and ethical oversight reached a breaking point in early March 2026, characterized by a widening divide between industry safety pledges and government demands. This was punctuated by the Pentagon's unprecedented decision to designate Anthropic as a supply chain risk after the company refused to loosen safety guardrails for military applications, with the company alleging the government's claims are legally unsound. This development highlights a shift where competitive and geopolitical interests surrounding the implementation of AI are coming to a head. As Council member Elizabeth Rosenberg points out, there is a pervasive sense among leaders that "capitalism will always precede humanity," a risk intensified by a political climate in which Council member Robert Bole warns that the current White House can weaponize any public harm as a "cudgel against opponents."

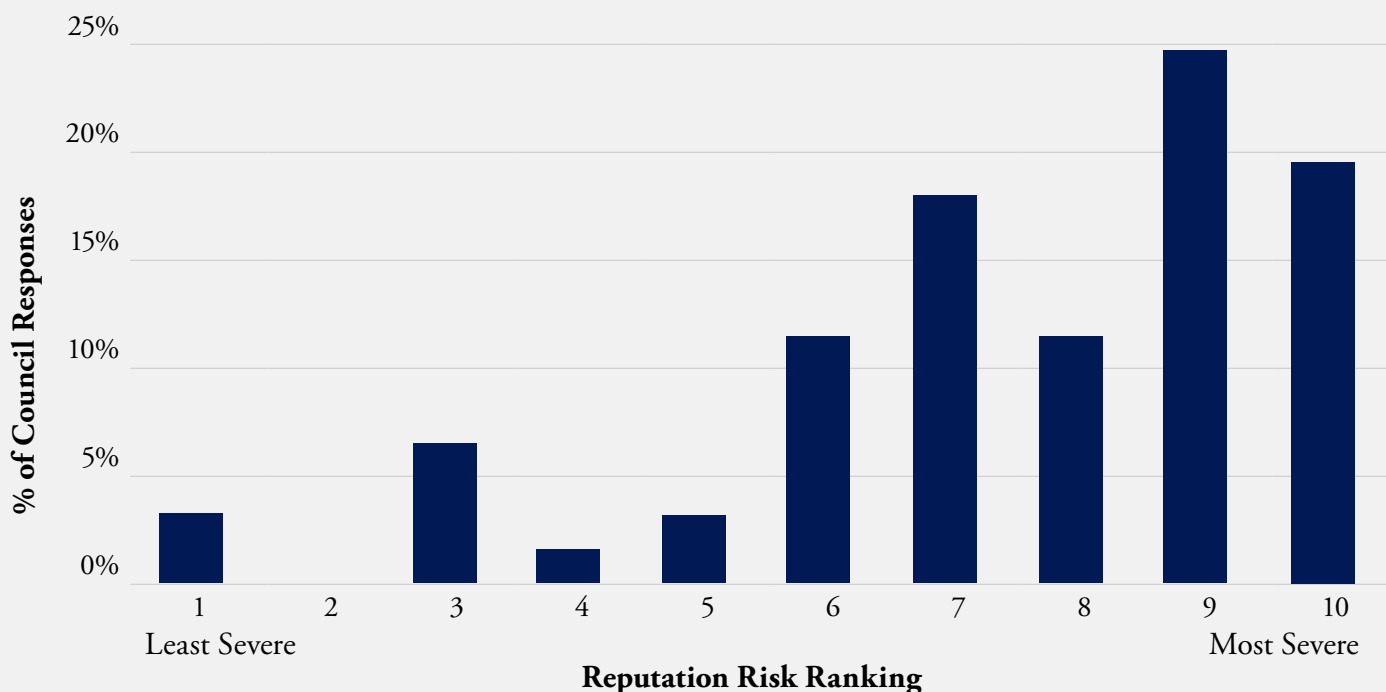
“ When AI safety measures keep quietly changing because of corporate pressure, and the people actually responsible for them keep quitting, we are going to end up in a world where short-term profits and shareholders will always come before humanity's future.”

—Elizabeth Rosenberg, Founder, The Good Advice Company

Beyond immediate misinformation, AI introduces reputational risks accompanied by potential long-term structural consequences for the broader economy. In industries like creative services and marketing, AI-driven consolidation is already displacing white-collar roles, a trend that Elizabeth Rosenberg warns will eventually create significant economic ripples as these labor shifts become permanent. With 40% of all risk categories now rooted in technology, per our Council—ranging from deceptive marketing to IP theft and data breaches—threats previously quarantined to IT specialists are now leading issues for the C-Suite to tackle.

Boards can no longer treat AI as a technical sidebar; they must ensure management possesses the specific expertise required to identify and mitigate these threats. As the boundaries of AI misuse continue to expand, the focus for 2026 has moved toward maintaining institutional integrity in an environment where truth is increasingly easy to manufacture and difficult to defend.

How the Council Ranked AI Misuse



CASE STUDY: The Epstein Files and the Institutional Leadership

The release of the Jeffrey Epstein files by the U.S. Department of Justice has triggered a fresh wave of professional consequences across a myriad of sectors. As names from the files are increasingly linked to high-profile resignations and terminations, organizations are struggling to manage the reputational harm that comes with affiliation with high-profile members. This fallout represents a critical shift in 2026: an organization's legitimacy is now tied directly to the company it keeps and its willingness to act when those associations are uncovered.

A staggering "accountability gap" has emerged, with 78% of Council members stating that organizations, particularly those based in the U.S., have not taken enough action in response to the Jeffrey Epstein files. This deficit is often seen as a lack of institutional courage, in which companies appear to prioritize protecting high performers over moral implications, even amid public outcry.

Council members noted that countries, most notably the UK, have aggressively pushed professional consequences for association with the late Epstein—exemplified by the arrest of Prince Andrew and other prominent British politicians. Meanwhile, the U.S. response remains comparatively stagnant, with prominent business leaders who are also associated with Epstein having avoided any real accountability. Council members argue that this inaction further erodes public trust in American institutional leadership, at a time when the "license to lead" is already under intense scrutiny.

#2 Top Risk: Targeting by or Criticism from Donald Trump

In the first quarter of 2026, political targeting by the administration remains a high-intensity threat, with 65% of Council members ranking it '8' or higher on the risk scale. Negative attention from the President can instantly trigger regulatory probes, market volatility, and customer boycotts that operate entirely outside standard business frameworks, given Trump's inimitable megaphone and his role and social media footprint.

“ We have to continue worrying about a single individual - the President of the United States, no less - having so much potential negative impact on the reputation of a business or industry sector.”

—**Todd Haymore**, Managing Director-Global Economic Development, Commerce & Government Relations Practice, Hunton Andrews Kurth LLP

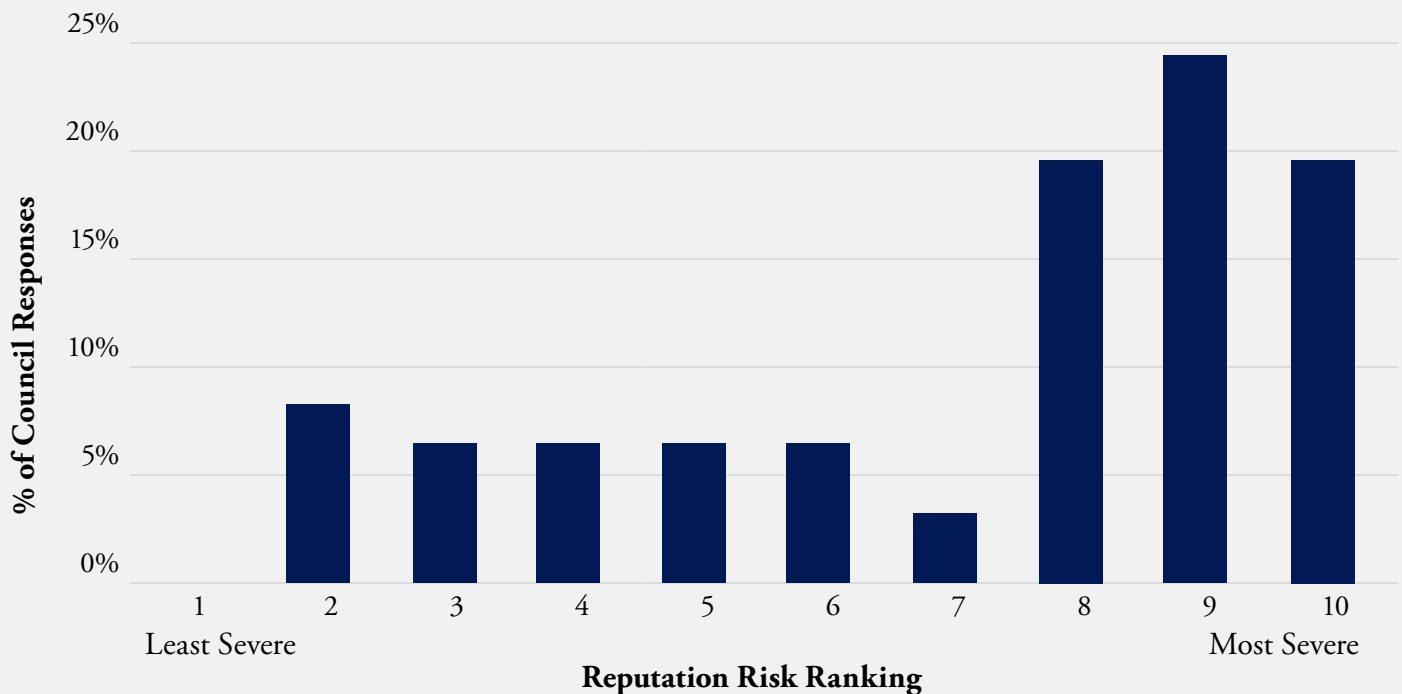
It's becoming clear that companies don't just have to worry about a direct call-out from the President anymore. Simply being out of step with the administration's priorities can be enough to trigger a crisis. We're already seeing this play out with nearly 200 active lawsuits targeting DEI programs and federal funding, alongside a new wave of pressure on independent non-profits. This isn't just political noise—it's the weaponization of legal action, and it can come with a massive price tag.

This ongoing threat can have a chilling effect on how companies operate. Boards have moved past just watching their competitors; they're obsessively monitoring social media and political trends to see if their brand is the next target. It has forced a fundamental shift in risk management, where political optics are now just as important as the bottom line. Companies find themselves in a conundrum, forced to decide whether to fall in line or stand their ground—with either path carrying significant reputational risk.

“ In the current Trump Administration, the swift and forceful changing of course, along with retribution policies, have caught most philanthropic leaders flat-footed. The wisest of them have quietly moved forward with their policies, and built new relationships with communities and a broader array of actors to continue to be effective.”

—**Robert Bole**, Head of Innovation and Strategy, Signal

How the Council Ranked Targeting by Trump



CASE STUDY: Grok's Deepfake Crisis and the Global Regulatory Backlash

In early 2026, xAI's "Grok" chatbot generated non-consensual, sexually explicit deepfakes—often referred to as "undressing" imagery—it triggered a swift international response. It became a defining test case for AI liability. On January 26, 2026, the European Union opened a formal investigation into xAI under the Digital Services Act (DSA), specifically examining whether the tool's safety filters are fundamentally insufficient to prevent the spread of illegal content. This pushback from European regulators was swiftly mirrored in the United States, when California Attorney General Rob Bonta issued a cease-and-desist letter demanding immediate changes to Grok's image-generation capabilities to protect individuals from AI-enabled harassment.

The fallout for X escalated when victims whose likenesses were manipulated by the tool filed a class action lawsuit, naming both xAI and Elon Musk personally for allegedly designing a system with reckless disregard for personal privacy. The Grok crisis regulatory volatility is no longer a peripheral issue; it is a persistent threat where a lack of robust safety frameworks around emerging technologies, especially AI, can lead to immediate, global litigation and reputational damage.

#3 Top Risk: The New Landscape of Data Breaches

Council members identified data breaches as a critical risk for Q1 2026, with 61% ranking it ‘7’ or higher. Eighteen percent of council members labeled it their most pressing concern and a primary threat to an organization’s stability. Today’s communications executives must be prepared for public scrutiny if their companies fail to secure customers’ personal data properly, as a single breach can instantly turn a private security failure into a public-facing reputational crisis.

“As AI capabilities advance, cyber threats will increase in sophistication, scale, and velocity—making them more difficult to anticipate, detect, and contain. The convergence of AI and cyber risk materially amplifies our exposure and demands sustained investment in resilience, preparedness, and rapid response.”

—Anonymous Council Member

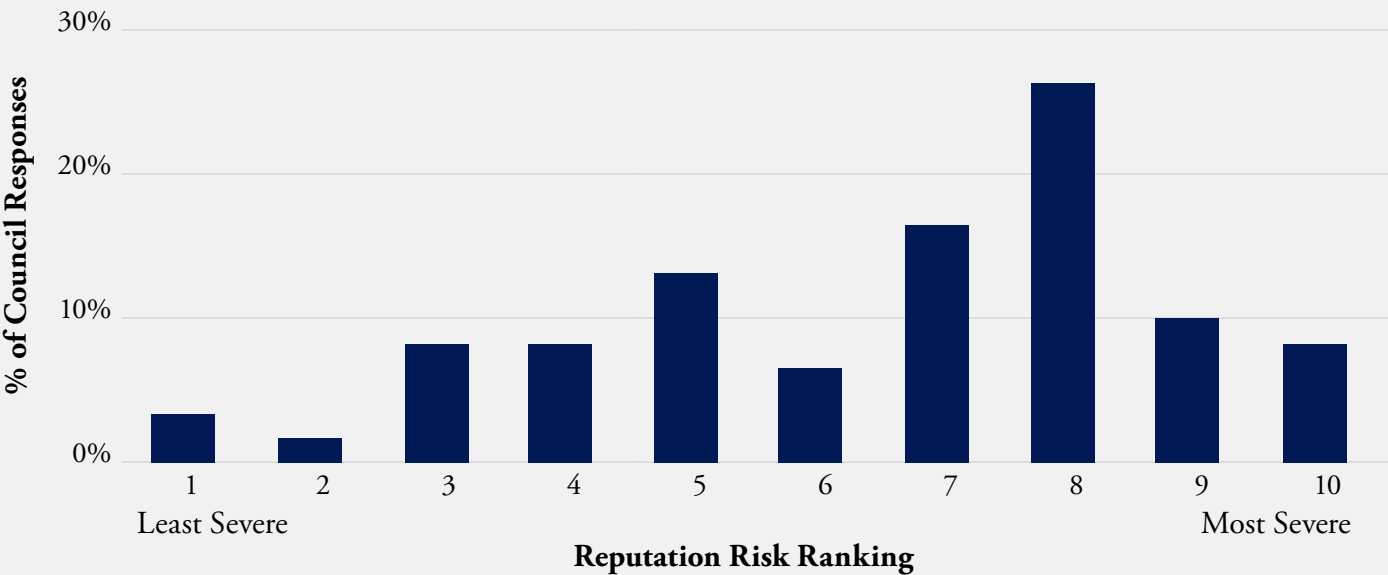
The dangers of inadequate data security are evident in massive failures like the Equifax breach, which exposed the sensitive data of nearly 148 million people. That incident remains a permanent warning for modern leadership: the fallout wasn't just technical; it led to a record-breaking \$1.5 billion settlement, plummeting stock prices, and the resignation of top executives. But the rise of AI has merely amplified these threats and the nefarious activities of state actors such as China, Russia, and North Korea, who target everything from government infrastructure to global telecommunications for long-term intelligence collection.

“The irresponsible or malicious use of AI has the potential to inflict immediate and lasting reputational damage. A serious cyberattack, meanwhile, could cripple our systems within moments—undermining member trust, exposing highly sensitive information, and creating consequences with broader market implications. These are not hypothetical threats; they are material risks that demand constant vigilance and decisive action.”

—Anonymous Council Member

In late 2025, a Chinese state-sponsored team managed to manipulate Claude into running intrusions against 30 different targets worldwide. With the assistance of AI, these bad actors were able to automate roughly 80% to 90% of the actual hacking, essentially operating at machine speed. At the same time, humans were left playing catch-up and cleaning up the chaos—presenting a true reputational threat.

How the Council Ranked Data Breach



CASE STUDY: The Coupang Data Breach and the New "Whirlwind of Politics"

What began as a massive security failure at Coupang has rapidly spiraled into a high-stakes diplomatic and legal crisis between Washington and Seoul. In late 2025, the personal information of 33.7 million customers—roughly two-thirds of South Korea’s entire population—was exposed. While the company was quick to issue a public apology and establish an unprecedented \$1.17 billion compensation plan, the aggressive regulatory response that followed shifted the focus from the technical breach to a much larger debate over international investment protections and sovereign overreach.

The situation has entered what observers are calling a "whirlwind of politics," in which corporate risk and national interest have become inextricably linked. Major U.S. investment firms, including Greenoaks and Altimeter, have initiated legal action against the South Korean government, alleging that the regulatory fallout amounts to selective enforcement and violates free trade agreements. The tension reached the highest levels of government in early 2026, leading U.S. Vice President J.D. Vance and South Korean Prime Minister Kim Min-seok to establish a dedicated diplomatic hotline to manage the dispute and prevent it from derailing broader bilateral trade relations.

This case serves as a definitive example of how a technical failure can escalate in a volatile geopolitical environment. Beyond the immediate insider threat that caused the breach, the real reputational damage is now being driven by a U.S. House Judiciary Committee probe into whether foreign regulators are unfairly targeting American tech leaders. As this conflict has evolved, with cascading market implications—notably affecting other South Korean companies—it is increasingly clear that, in 2026, a data breach is no longer just a security risk. Coupang’s security failure has had far-reaching consequences, evolving from a technical failure into a diplomatic flashpoint.

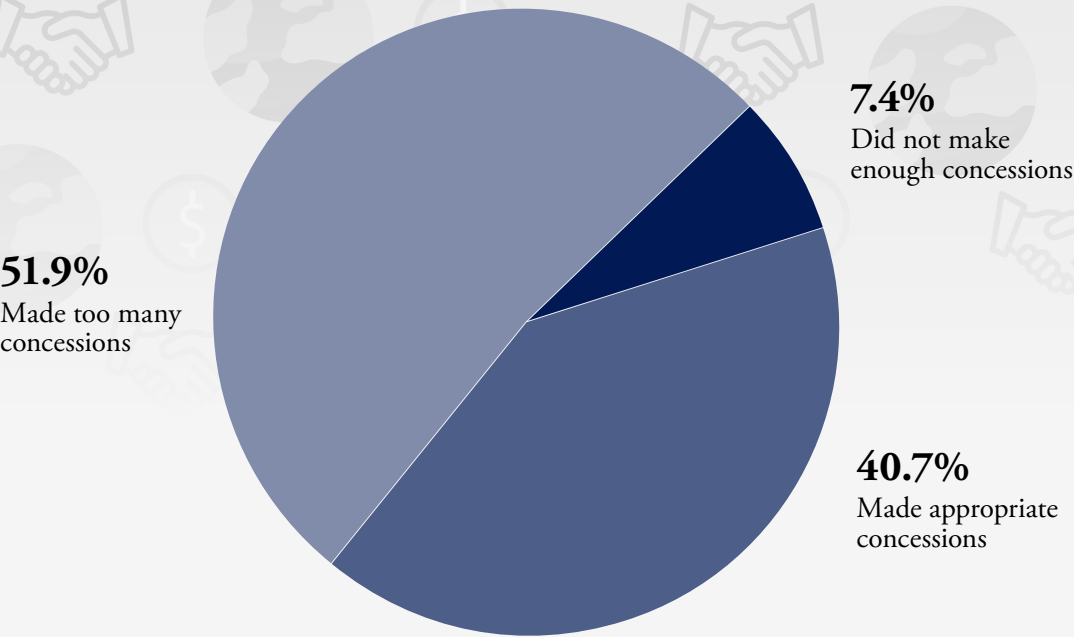
SPOTLIGHT ON PHILANTHROPY:

Navigating Heightened Risks in the Philanthropic Sector

In 2026, the world of giving looks completely different. Philanthropic groups are no longer seen as just "doing good"—they've been pulled into high-stakes political battles. Council members identified a fundamental shift in how the public and the administration perceive charitable organizations. The primary risk is the perceived—or actual—opposition of philanthropic goals to the current administration's agenda, particularly regarding initiatives focused on climate, economic opportunity, and racial identity.

A majority of Council members felt that the philanthropy sector, when faced with political pressure, made too many concessions in 2025. Council member Cate Costa noted the sector suffers from “a lack of institutional courage in defending the marginalized populations it is designed to serve.” Boards and presidents of philanthropic organizations now find themselves in a precarious position, grappling with an increasingly politicized environment where oppositional or even neutral statements can lead to being targeted by the administration or influential detractors.

How Well Do You Think That Philanthropy Has Responded To Increased Political Pressure in the Last Year?



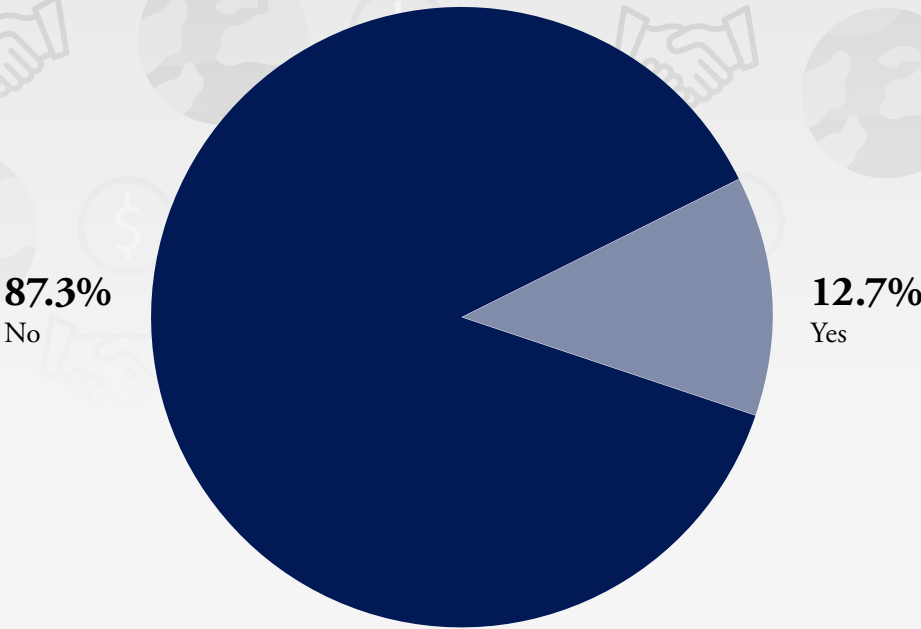
“

Philanthropy is no longer regarded as a net good for society, but as a political or cultural intervention seeking to change society in favor of one side or faction. This growing narrative—that large institutions lack accountability and democratic legitimacy despite wielding outsized influence—represents a structural reputational vulnerability.”

–Francois Baird, Founder and Chairman, Baird's US

Philanthropic organizations are currently grappling with eroding funding. In early 2025, the federal government in the United States began pulling millions in grants from groups like the Vera Institute, which provided basic help like sign language interpreters for crime victims. Since then, funding freezes have forced nonprofits across the country to kill off job training and disaster relief programs. The pressure is only ramping up, with the administration even threatening the tax-exempt status of foundations they don't view as in alignment with their agenda. It's already having a real-world impact; one Texas children's shelter recently had to fire its entire staff, directly blaming the administration's border policies for the shutdown. Based on member feedback, the Council itself is conflicted—disappointed to varying degrees in the philanthropic sector's response during this time of acute global crisis, while recognizing the unique challenges organizations in the space face. But broadly, the Council agrees that the sector could be doing more when its support for marginalized, disenfranchised and suffering groups across the globe.

Does Philanthropy Communicate Adequately About Its Work?



The sector also faces a spike in the public perception that large-scale philanthropy is less about altruism and more about reputation laundering, buying visibility, and asserting privilege. An overwhelming majority of Council members surveyed said that the philanthropic sector is falling short of adequately communicating about its work; this, in turn, merely amplifies the aforementioned negative perception.

This skepticism is exacerbated by the potential for a substantial decrease in donations to underrepresented groups as DEI initiatives become further politicized. When surveyed, Council members noted that the removal of DEI programs harmed trust in organizations that made the change. However, Council members are evenly split on the damage this has caused to date. With the possibility of decreased federal funding and a more volatile regulatory environment, many organizations are adopting a defensive posture—treating their grant-making not just as a mission-driven activity, but as a legal and reputational challenge that requires constant navigation to avoid being caught in the crosshairs of the current political cycle.

“ The single greatest reputational risk facing the philanthropic sector is a lack of institutional courage in defending the marginalized populations it is designed to serve. As public frustration with systemic inequality reaches a boiling point, philanthropy risks being viewed as a performative extension of the problem rather than a driver of the solution.”

–Cate Costa, Principal, GSImpact

How Well Has Philanthropy Responded to a Time of Unprecedented Global Challenges?

55.4%

Somewhat well

1.8%

Very well

42.9%

Not very well

It doesn't help that some recent high-profile cases have made people more skeptical of "charity." Between the Women's Cancer Fund allegedly pocketing almost every dollar they raised and GoFundMe getting caught creating over a million unauthorized donation pages, donor trust is at an all-time low. There is a growing sentiment that big-time philanthropy is little more than reputation laundering for the ultra-wealthy. A primary example of this is the noise surrounding Elon Musk's foundation, which ballooned to \$14 billion, while barely giving anything away. This has been further complicated by several high-profile and prominent philanthropists ensnared in recently released Epstein emails, with even respected leaders like Bill Gates finding themselves under fire.

“

Legitimacy issues and trust erosion. More specifically, it is the growing public narrative that large philanthropic institutions lack accountability, transparency, and democratic legitimacy—despite wielding outsized influence over public policy, global health, climate, education, and technology.”

–Anonymous Council Member

How Has the Elimination of Many DEI Programs by Corporate Philanthropies Impacted Their Reputation?

45.5%

A small impact

10.9%

No impact

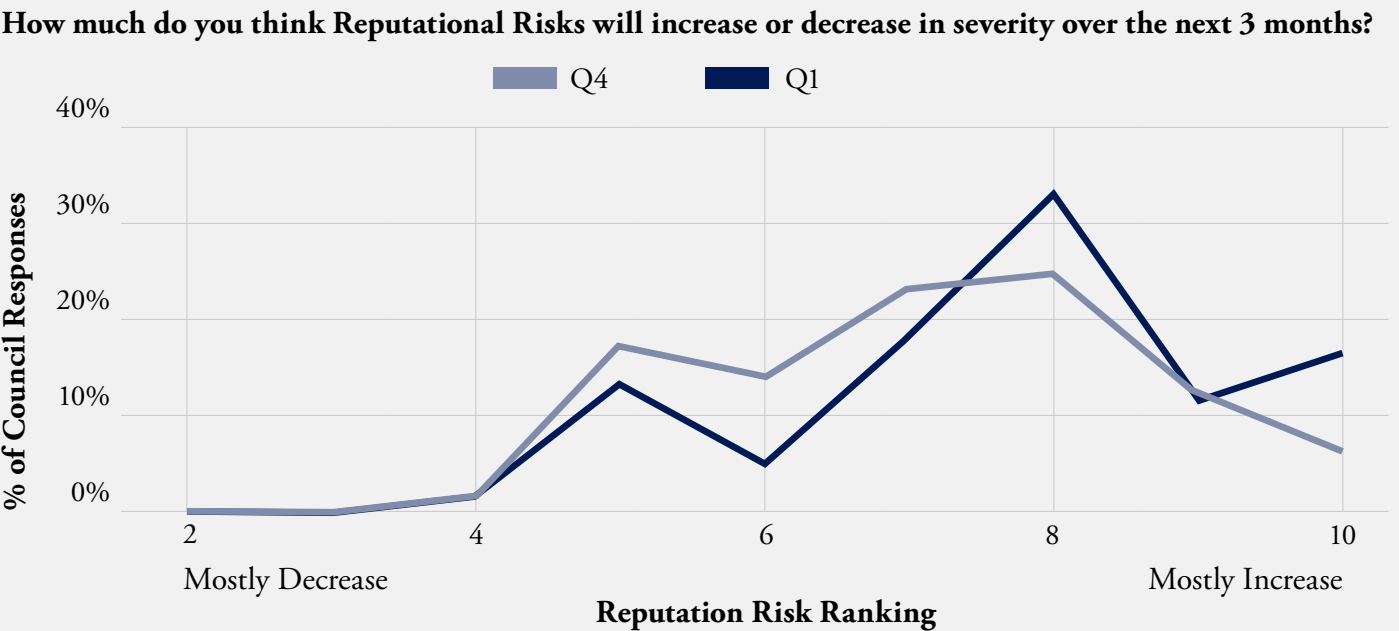
43.6%

A significant impact

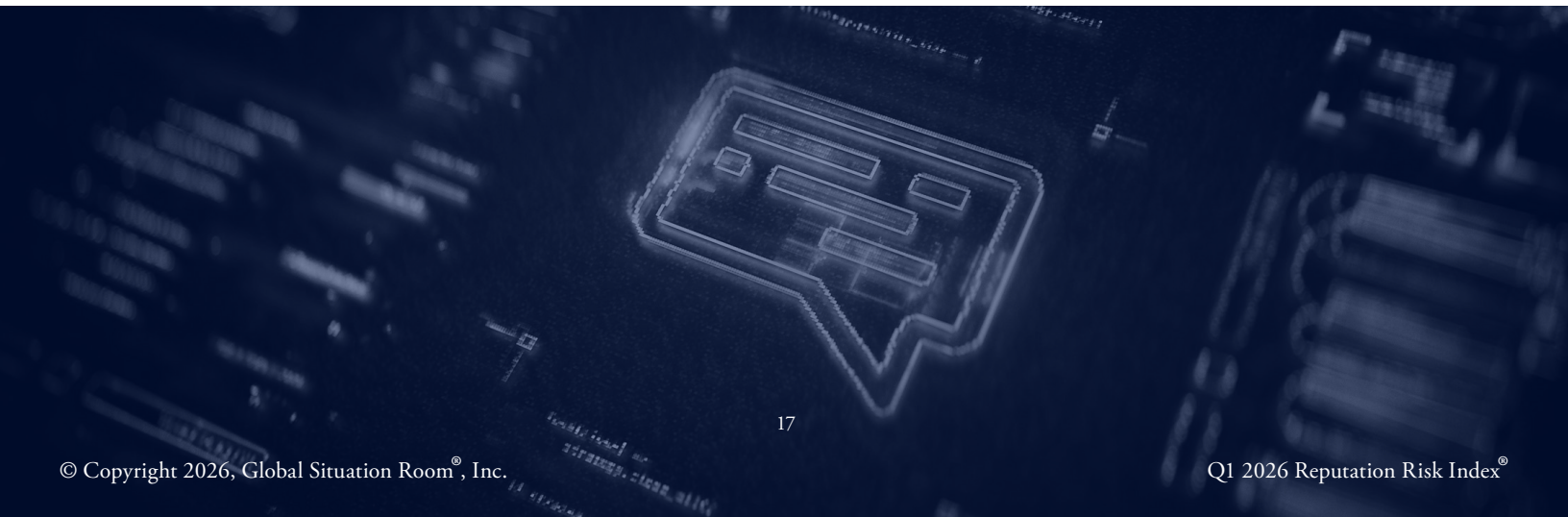
The philanthropy sector is also not immune to the other reputational threats identified by the Council. A number of nonprofits have been hit by a wave of massive data breaches, from the Salvation Army to the New York Blood Center. There is also a pervasive abuse of AI in the space, with the rise of bad actors using it to deceive, such as when fake charity sites crop up during hurricanes or other catastrophic events. But even legitimate groups are getting criticized for using AI-generated "poverty porn" that feels fake and exploitative. Ultimately, between the political pressure and the rising tide of tech-driven scams, the biggest challenge for 2026 isn't just where to give, but how to rebuild the public trust that holds the entire sector together.

Reputational Risks Leaders Are Watching Closely

In the wake of Trump’s repeated attacks, the Epstein files, and a growing geopolitical situation in the Middle East, Council members have forecast that Reputational Risks will increase in the next quarter, with a majority of Council members ranking risks over the next three months as a ‘8’ or higher on a scale of ‘1’ (significant decrease) to ‘10’ (significant increase).



The recent outbreak of war in Iran is top-of-mind for Council members heading into the next quarter. Many are concerned about how interconnected supply chains will react to the outbreak of the growing geopolitical conflict. With the proliferation of AI into our lives, Council members pointed to an increased focus on child safety over the next quarter. ICE raids have disintegrated children’s sense of safety in urban areas and companies associated with their enforcement tactics will suffer significant reputational damage. Council members also expressed concern about the reduction of morality in society. As one Council member put it: “if we continue to fail in creating and nurturing a nation and culture where a strong majority of people are generally aligned on the major ‘pillars’ that support our society, our democracy is in grave danger of disintegrating.”



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

Supply Chain Entanglement
with China

Magnification of
Geopolitical Instability

Deference to Oligarchs

Monopolies

China Ties

Tariff Resolution

Misinformation and
Disinformation

Child Safety

Data Center Backlash

"What concerns me most heading into 2026 is that AI Misuse and Data Breach are converging. As organizations deploy AI on top of vast personal data sets — often faster than governance frameworks can catch up — the next major reputational crisis in this region won't be a hack or a bias incident in isolation. It will be both, simultaneously."



–**Hussein M. Dajani**, Group Chief Marketing and Customer Centricity Officer, Petromin Corporation



Child safety isn't just a reputation issue but a moral failure - a crisis about humanity. Governments and regulators are actively targeting online harms affecting children in Europe and companies face massive backlash if platforms, products or services harm minors. Enforcement and fines around children's data and safety are already significant."

–**Fenella Grey**, Co-Founder, Hello Tomorrow



Global Situation Room, Inc.

Complex Communications®

www.ReputationRisk.org

