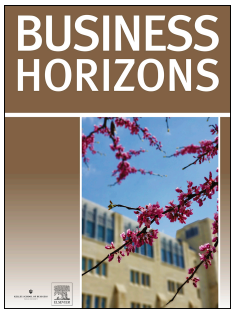

Managing spillover crises in the age of generative AI

Yijing Wang, Daniel Laufer

PII: S0007-6813(25)00173-9

DOI: https://doi.org/10.1016/j.bushor.2025.10.006

Reference: BUSHOR 2105

To appear in: *Business Horizons*

Please cite this article as: Wang Y. & Laufer D., Managing spillover crises in the age of generative AI, *Business Horizons*, https://doi.org/10.1016/j.bushor.2025.10.006.

BEYOND THE HORIZON

Managing spillover crises in the age of generative AI

Yijing Wang*, ^
Department of Media & Communication, ESHCC
Erasmus University Rotterdam
Burgemeester Oudlaan 50
Rotterdam
South Holland, 3062 PA
The Netherlands
y.wang@eshcc.eur.nl

Daniel Laufer ^
School of Communication Studies
Auckland University of Technology
55 Wellesley Street
East Auckland City
New Zealand
dan.laufer@aut.ac.nz

***Corresponding author**
^ **Author Contribution Statement:** Both authors contributed to this article equally.

Managing spillover crises in the age of generative AI

Abstract

The rapid development of generative artificial intelligence (GenAI) has marked a significant shift in how organizations operate and innovate. While GenAI offers new opportunities, it has also created new risks that can escalate into crises. Importantly, these crises are not always limited to the organization where they originate but can spill over to other organizations in the same sector, leading to broader reputational consequences. This article investigates such spillover crises in the age of GenAI. We build on Laufer and Wang's crisis spillover model and extend it to GenAI-related contexts. Specifically, we identify five types of spillover crises associated with GenAI and illustrate them through real-world cases. These cases highlight how reputational damage can extend beyond a single firm, affecting others in the industry. We propose a strategic framework to help organizations identify the risk of spillover crises, and we offer prescriptive guidance for avoiding, mitigating, or responding to spillover crises when they occur.

KEYWORDS: Crisis spillover; Generative AI; Crisis types; Reputational damage; Crisis response strategies

1. Spillover crises in the age of generative AI

The rapid development of generative artificial intelligence (GenAI) technologies has marked a significant shift in how organizations innovate and deliver value (Kaplan & Haenlein, 2020). From GenAI-generated content in marketing and journalism to autonomous decision-making systems in the hiring process and healthcare, GenAI has rapidly transitioned from experimental novelty to core business infrastructure, widely adopted across different sectors (Holmström, 2022). As this trend intensifies, risks sparked by GenAI failures are unavoidable, and they may not always be confined to the organization where the incident originated, but can result in crisis spillover, adversely impacting other organizations in the same sector (Chang & Rim, 2024; Laufer & Wang, 2018).

For example, in 2023, *Sports Illustrated* faced public backlash after revelations that it published GenAI-generated articles using fake author profiles. Although the crisis only involved *Sports Illustrated*, the resulting uproar quickly spread to other media outlets, triggering industry-wide scrutiny of editorial authenticity (Salam, 2023). Similarly, in the same year, *Levi Strauss*' announcement about the use of GenAI-generated virtual models led to widespread concerns about the displacement of human labor in the fashion industry, adversely impacting other fashion brands in the industry (Savage, 2024). In both cases, the reputational damage spread beyond the directly impacted organization, illustrating the phenomenon of crisis spillover at the industry level in the age of GenAI.

Laufer and Wang (2018, p. 174) defined crisis spillover risks as arising when "consumers make assumptions of guilty by association," and proposed a model based on the accessibility-diagnosticity framework from the field of psychology. Further, Wang and Laufer (2024) argue in their cross-disciplinary review article that there is growing relevance of the crisis spillover phenomenon in an era where organizations are increasingly dependent on digital technologies. In this article, we investigate how GenAI-induced crises can lead to crisis spillover effects across organizational boundaries. Our contributions are fourfold. First, we extend the crisis spillover model proposed by Laufer and Wang (2018) to an under-researched area of great importance in the age of GenAI, i.e., GenAI-related crises. Second, we identify five types of spillover crises associated with GenAI, and we explain through real-world examples how such crises can affect other GenAI-integrated organizations in an industry that are not always directly involved in the crisis. Third, we propose a strategic framework for companies to protect themselves if they are at risk of a GenAI spillover crisis. Fourth, we offer strategies that practicing managers can use to effectively avoid, mitigate, and respond to spillover crises.

2. Revisiting the crisis spillover model

In their *Business Horizons* article, Laufer and Wang (2018) explained that crisis spillover occurs when a crisis triggers broader awareness to stakeholders beyond the organization experiencing the crisis and is perceived as diagnostic of an issue affecting a shared category, such as industry or organizational type. Their perspective is derived from the accessibility-diagnosticity framework (Feldman & Lynch, 1988; Roehm & Tybout, 2006).[1] The framework is highly relevant for understanding spillover risks in the age of GenAI. For example, when

[1] In this framework, accessibility refers to how easily consumers can recall and associate the focal firm with the one experiencing the crisis. In other words, this occurs when an organization shares a common category such as an industry or organizational type. Diagnosticity, on the other hand, occurs when the attributes of the crisis are perceived as indicative of a category-wide problem. In other words, there is a perceived fit between the crisis type and the category.

GenAI-generated content misleads consumers or an algorithm demonstrates bias, the public may infer that these are not isolated incidents but rather structural issues intrinsic to the technology or the organizations deploying it (De Freitas, 2025). When companies share one or more of the risk factors associated with shared categories, such as industry, organizational type, country of origin, or positioning strategy, they are more likely to be implicated through guilt by association (Laufer & Wang, 2018; Wang & Laufer, 2024).

In the digital age, where information spreads rapidly and public narratives coalesce online, the risk of being judged as guilty by association has only intensified (Laufer & Wang, 2024). For example, consider the role of industry as a crisis spillover factor: A crisis involving the displacement of human labor at one fashion company may activate broader concerns about bias in all fashion brands using GenAI systems. The *Levi Strauss* scandal mentioned earlier illustrates such a crisis spillover effect. Organizational type further complicates matters. For example, nonprofits that leverage GenAI to increase operational efficiency may be lumped together if one is implicated for privacy violations, even if others adhere to stringent data ethics. For instance, a recent news article mentioned that when the NGO *EyesOnOpenAI* challenged *OpenAI* over transparency in its nonprofit governance, many observers began to question public trust not just in *OpenAI* but in nonprofit-led AI initiatives broadly, worrying that nonprofit structures may mask profit motives or lax oversight (Johnson, 2025). As Laufer and Wang (2018) and Wang and Laufer (2024) argue, comparable organizational missions and perceived motivations can amplify the accessibility of a crisis. Similarly, the same country of origin may shape public expectations about corporate behavior and technical standards due to high accessibility through a shared category. For example, a GenAI-related scandal at a *Silicon Valley* firm around privacy could spill over to other American technology companies due to pre-existing beliefs about U.S. firms prioritizing innovation over data security (Maher & Singhapakdi, 2017). This was illustrated when Italy's privacy watchdog fined *OpenAI* for ChatGPT's violations in collecting users' personal data. This resulted in broader concerns in Europe of OpenAI and other American technology companies' privacy violations (Zampano, 2024).

Perhaps equally subtle, yet particularly insidious, is the dimension of strategic positioning argued by Laufer and Wang (2018) as a key crisis spillover factor. For example, when organizations publicly align their brand with values such as trust, transparency, or digital innovation, they increase the likelihood of being perceived as similar to other companies with a comparable positioning strategy. This is especially relevant in the context of GenAI. Increasingly, companies across sectors are positioning themselves as "GenAI-driven" or "GenAI-enhanced," framing the adoption of GenAI as a marker of technological leadership and a differentiating factor in their industry (De Freitas, 2025). While this alignment may yield reputational benefits under normal conditions, it also introduces a shared identity that heightens accessibility in the event of a crisis. In other words, organizations that prominently market their use of GenAI may find themselves lumped together in public perception when one firm faces scrutiny. The crisis no longer appears isolated. Instead, it reinforces a broader concern about the risks or ethics of GenAI adoption, thereby increasing the spillover potential to competing companies that share a positioning strategy around GenAI. For example, after the FTC sued Air AI for advertising exaggerated business outcomes tied to its GenAI tools, media coverage and public commentary began assessing not just Air AI but many GenAI-firms making similar growth or earnings claims (Drayton, 2025). This raised trust issues across companies with a similar strategic positioning.

According to the crisis spillover model (Laufer & Wang, 2018; Wang & Laufer, 2024), the spillover effect becomes particularly pronounced when companies share multiple risk factors, such as being in the same industry and pursuing a positioning strategy around GenAI (e.g., GenAI-driven or GenAI-enhanced). In such cases, their perceived interconnectedness creates a cognitive shortcut for consumers, media, and stakeholders to draw guilt-by-association conclusions. As Laufer and Wang (2018) suggest, the more nodes of similarity between organizations in the public's mindset, the higher the accessibility, and thus the greater the risk of crisis spillover effects.

3. GenAI-related crises with spillover risks

While accessibility, or belonging to a shared category, is a key component in determining whether a crisis will spill over, it is not sufficient on its own (Laufer & Wang, 2018). The potential for crisis spillover also depends on diagnosticity. As noted earlier, this refers to whether the attributes of a specific crisis are perceived as symptomatic of a broader category-level problem (Feldman & Lynch, 1988; Roehm & Tybout, 2006). A crisis perceived as highly diagnostic signals to stakeholders that the issue is not a one-off failure but reflects systemic flaws in the underlying technology or organizational practices that impact a broader category. Accordingly, we identified five types of GenAI-related crises that are high in diagnosticity and thus pose elevated spillover risks for AI-integrated organizations: *authenticity/integrity, labor displacement, technical failure, data security and privacy, and discrimination/bias* (see Table 1). We focused on these five types of risks because they mirror the most immediate concerns executives and stakeholders raise when it comes to GenAI adoption. As Kunz and Wirtz (2024) point out, companies are expected to take responsibility for digital practices across the board, meaning that failures in areas such as authenticity, privacy, or bias are quickly seen as systemic weaknesses rather than isolated errors. Bowen (2024) similarly observes that, without clear ethical standards (e.g., relating to labor displacement, technical bias, or failure), many stakeholders assume that firms will pursue any technological possibility unless they prove otherwise. This mindset makes crises in these domains especially dangerous. They not only damage the company directly involved but also signal to the market and the public that other companies belonging to the same category (e.g., in the same industry) may be at risk. Thus, these five areas mentioned above carry heightened spillover potential since they touch on widely shared concerns about how GenAI is used responsibly in business. Each crisis type is described below using real-world examples that show how high diagnosticity amplifies guilt-by-association beyond the initial focal organization for a GenAI-related crisis.

It is worth noting that a key factor in the diagnosticity of all of these spillover risks is the perception by stakeholders that GenAI solutions are viewed as a homogeneous group (De Freitas, 2025). Unlike solutions involving people, which are viewed as varied and heterogeneous, researchers have found that GenAI solutions are viewed as sharing similar characteristics (Longoni et al., 2022), which makes GenAI-related crises more prone to spillover to other GenAI-integrated organizations.

3.1. Authenticity/Integrity crises

GenAI-related crises that adversely impact the perceived authenticity or integrity of an organization's communications strike at the very heart of public trust (Deptula et al., 2025). In the 2023 *Sports Illustrated* example described earlier, the company was criticized for publishing GenAI-generated articles under fabricated author identities (Salam, 2023). Although the media company claimed editorial oversight, the crisis triggered a wave of

skepticism about the legitimacy of GenAI-generated content across the entire journalism industry. Other media companies (e.g., *BuzzFeed*) that incorporated GenAI faced scrutiny, not necessarily because of *their* practices, but because the crisis at *Sports Illustrated* was perceived as an industry-wide crisis.

Another example of how a crisis related to authenticity and integrity can spillover to other organizations is the use of GenAI-generated images by the Ai Yixing Public Welfare Service Center in Chengdu, China, for donation appeals in 2024 (Huang, 2024). The organization was criticized for presenting computer-generated images of beneficiaries as though they were real people, raising concerns that donors were being misled about the impact of their contributions. Although the crisis initially centered on this single organization, it quickly ignited a broader debate about whether other charities might also be fabricating or exaggerating their appeals with GenAI tools. Journalists and watchdog groups began scrutinizing the fundraising materials of other charitable organizations in China, questioning whether they too might be misrepresenting reality (Huang, 2024). In this way, a localized GenAI-related crisis for one organization spilled over into a sector-wide challenge, amplifying concerns about authenticity and integrity across charities in China and undermining public trust in donation campaigns more broadly.

These two examples satisfy the two key conditions of the accessibility–diagnosticity framework. Accessibility is high because the affected organizations share strong categorical similarities with others in their sectors, such as media companies or nonprofit charities, making it easy for stakeholders to cognitively form a link. Diagnosticity is also high, as both crises tap into foundational societal concerns related to GenAI use, including credibility and transparency that are viewed as systemic, rather than isolated. According to the crisis spillover model, when a single organization's crisis is perceived as reflective of industry-wide practices or ethical blind spots, the reputational harm is likely to spill over to similar organizations. In media companies and nonprofit organizations, for example, the convergence of shared missions, communication methods, and public-facing narratives amplifies the potential for guilt-by-association, making authenticity/integrity crises a high risk for spillover in the age of GenAI.

3.2. Labor displacement crises

Similar to authenticity/integrity crises, crises involving the perceived displacement of human labor by GenAI often result in societal debates over the future of work (Chen et al., 2022; Chhibber et al., 2025). As a result, these crises are highly diagnostic as well. A case in point is *Levi Strauss*' 2023 announcement to collaborate with *Lalaland.ai* to introduce GenAI-generated fashion models in its advertising campaigns (Savage, 2024). While the company framed the move as a step toward inclusivity and efficiency, critics accused the company of attempting to lower costs by hiring fewer models, particularly among underrepresented groups in the fashion industry (Greene, 2024). The controversy quickly extended beyond *Levi*'s to other fashion brands such as *Target*, *Kohl's*, and fast-fashion giant *Shein*, as it raised normative concerns about the ethics of AI-driven visual communication.

Another illustrative case arose in the customer service sector. In 2023, major corporations such as *British Telecom* announced plans to replace significant portions of their call-center workforce with GenAI-powered chatbots (Sweney, 2023). While these companies promoted the technology as a way to improve efficiency and reduce wait times, unions and employees denounced the move as a cost-cutting strategy that sacrificed jobs and service quality. Public backlash intensified when customers complained about the inability of GenAI chatbots to

resolve complex issues, amplifying concerns that GenAI adoption would both degrade consumer experience and accelerate large-scale labor displacement. As with the *Levi Strauss* case, criticism extended well beyond the companies directly involved. Other companies, such as Vodafone, were affected. This fueled broader debates about the ethical and economic implications of automating frontline service roles across industries.

According to Laufer and Wang's (2018) crisis spillover model, accessibility in these cases is driven by shared public narratives around digital transformation in fashion and customer service. Diagnosticity is high because the backlash was not merely about *Levi*'s or the telecommunications companies' choices, but about broader fears of automation displacing human creativity and labor, perceived as an industry trend rather than an isolated act. The positioning of many fashion brands and service providers as progressive and customer-oriented further amplified their similarity in the public's mind.

3.3. Technical failure crises

The third crisis type we identify is technical failure. Crises stemming from such failures of GenAI systems often signal systemic design flaws or a premature rush to deployment of GenAI tools (Kaplan & Haenlein, 2020), making them highly diagnostic. A good example of this type of crisis is the damage suffered by an autonomous vehicle company operated by *Cruise*, a robotaxi subsidiary of *General Motors*, after one of its cars failed to recognize a pedestrian at night, resulting in a serious injury (De Freitas, 2025). Although the incident involved a single vehicle, public attention quickly expanded to include other self-driving tech firms, particularly those using similar LLM-*driven* perception models. Media outlets highlighted similarities in the underlying GenAI systems across companies, while experts pointed to the "black box" nature of machine learning as a structural weakness rather than a firm-specific error. The failure was perceived not as an isolated incident, but as evidence that GenAI-based systems may be fundamentally ill-equipped to handle complex cases in real-world environments. The spillover effect from this crisis led to regulatory delays and a drop in the stock prices of competing firms such as *Waymo* and *Zoox*, even though they did not experience any safety incidents. Moreover, cities that had been negotiating pilot projects with other robotaxi providers temporarily suspended approvals, and insurance companies like *Swiss Re* reconsidered liability frameworks for autonomous driving. This reinforced the impression that the *Cruise* accident was not simply a single-point failure but indicative of an industry-wide fragility in GenAI deployment.

Another example of a spillover crisis related to a technical failure that happened in the higher education sector (Staton, 2023). Following widespread adoption of GenAI-based detection tools meant to flag ChatGPT-assisted plagiarism, universities in the UK, including Cambridge and other leading UK universities, began encountering alarming false positives, especially among non-native English-speaking students. In one widely publicized case, a student was falsely accused of using AI to write a philosophy paper, only to later be cleared, after weeks of reputational damage to the university and emotional distress to the student. A major factor in the spillover effect of the crisis to other universities was the use of GenAI detection tools. As previously mentioned, GenAI tools are perceived by stakeholders to be homogeneous, causing the crisis to spill over to other universities, even if they used other types of GenAI tools to identify plagiarism. The narrative quickly shifted from isolated implementation flaws to a broader question of whether universities were blindly outsourcing judgment to unproven GenAI.

In these two cases, like the previous ones, the *accessibility–diagnosticity* framework offers a powerful explanation of how these crises spilled over to other firms. Accessibility is high because the implicated organizations share common categories with the organizations experiencing the crisis—industry and the deployment of GenAI. Diagnosticity is also high, since both crises cast doubt on the core functionality and maturity of GenAI technologies themselves. This occurs because stakeholders view these failures as emblematic of broader issues, as GenAI solutions are perceived to be part of the same technological ecosystem.

3.4. Data security & privacy crises

Crises involving GenAI and data governance frequently evoke concerns about surveillance and institutional accountability (Prahl & Goh, 2021), making them diagnostic of organizational control or lack thereof. In 2023, New Zealand's *Ministry of Business, Innovation and Employment* banned the use of ChatGPT and other GenAI tools by staff, citing concerns over data leaks and third-party access to sensitive information (Cardwell, 2023). Although the move applied to a specific government body, it fueled broader discussions about the risks of integrating GenAI tools into administrative and enterprise systems without robust security protocols at other government ministries.

Similarly, in the same year, *Samsung* faced a crisis when engineers inadvertently input sensitive source code and confidential meeting notes into ChatGPT while troubleshooting errors (Ray, 2023, May 2). These disclosures, although unintentional, immediately raised alarms about how easily proprietary corporate data could be shared with external GenAI systems outside of a company's control. In response, *Samsung* swiftly banned the internal use of ChatGPT and similar tools while exploring the development of its own in-house GenAI solutions. The case did not remain confined to *Samsung*; rather, it triggered broader anxieties across the technology sector about the risk of unmonitored employee interactions with public GenAI platforms, reinforcing fears that any firm allowing such practices might face comparable breaches of confidentiality and intellectual property.

With data security and privacy crises, diagnosticity is high because the incident raises red flags about systemic data vulnerability, suggesting that any organization using similar tools may be exposed to comparable threats. Meanwhile, accessibility stems from similarities in institutional type (e.g., government bodies, corporations, or nonprofits) using third-party GenAI systems, often under similar assumptions of trust. When one prominent organization publicly bans or discredits a GenAI tool, other adopters are cognitively clustered as facing the same risks, leading to a spillover in stakeholder concern even when no direct incident has occurred elsewhere. The *Samsung* case further demonstrates that even when the original breach is limited to one organization, stakeholders quickly generalize the perceived vulnerabilities to the wider industry, amplifying the spillover effect. Once again, the perceived homogeneity of GenAI solutions by stakeholders increases the likelihood that a spillover effect will occur.

3.5. Discrimination & bias crises

Last but not least, crises involving algorithmic bias, particularly in hiring and resource allocation, are an area of key concern. For example, *Amazon*'s discontinued AI recruitment tool was found to penalize women based on historical training data, systematically downgrading résumés that included terms such as "women's chess club captain" (Dastin, 2018). Similarly, *Workday* was recently sued for alleged racial and disability discrimination by its resume-screening algorithms, with plaintiffs claiming that qualified candidates were unfairly excluded from hiring pools and raising questions about the opacity of third-party AI

tools used in human resources (Wiessner, 2024). Both cases not only damage the reputation of the firms involved but also evoke widespread concern about systemic discrimination embedded in GenAI-based decision-making across the sector, particularly in contexts involving fairness and equity.

Diagnosticity in these cases is high, as stakeholders interpret such failures as structural (i.e., reflecting the biases and blind spots of the teams from the same industry designing and deploying these tools). Accessibility is heightened when multiple firms in the sector use similar tools (e.g., algorithmic resume screening), especially in regulated domains like employment or finance. As Laufer and Wang (2018) note, when public narratives coalesce around a few high-profile failures in one sector, other companies in the sector, even those with better controls, are pulled into the same reputational narrative. The result is a heightened risk of sector-wide trust erosion and crisis spillover, especially in industries already scrutinized for lack of diversity and inclusivity.

In summary, identifying these five high-diagnosticity crisis types has practical value for organizational risk and crisis communication strategies. While accessibility determines whether an organization can be perceptually linked to another's crisis, diagnosticity shapes the intensity and breadth of reputational spillover (Laufer & Wang, 2018; Wang & Laufer, 2024). Each crisis type triggers distinct stakeholder concerns—credibility, labor norms, system reliability, governance integrity, and social justice—thus widening resonance. Recognizing these distinctions enables firms to anticipate potential crisis spillover risks and tailor responses strategically. Thus, understanding diagnosticity empowers organizations to more precisely assess spillover risks and craft nuanced communication strategies for resilience in a GenAI-intensive ecosystem.

[Insert Figure 1 About Here]

We recommend managers begin identifying potential spillover risks based on the accessibility-diagnosticity framework. The 2x2 matrix in Figure 1 can be used to guide the severity of this risk. If organizations are facing spillover risks that fall into the five types identified in this article, managers will want to be especially vigilant. After identifying the most vulnerable areas, managers should collect data to assess whether spillover is occurring. As Laufer and Wang (2018) pointed out, gathering data from the news media and social media accounts that mention a GenAI-related crisis is occurring at other companies can provide strong evidence for managers that a potential spillover effect is likely.

4. Responding to AI spillover crises

When the spillover risk is high based on the accessibility/diagnosticity framework, and an organization has confirmation of spillover from the news media or social media, it is important for the organization to protect itself. According to Laufer and Wang (2018), an effective strategy to manage a spillover crisis is to differentiate the company from the organization experiencing the GenAI-related crisis. A good example involves crises associated with discrimination and bias. ChatGPT has been accused in the media of providing results to prompts that are biased (West, 2023). Claude, a competitor to ChatGPT, differentiated itself from ChatGPT by stating that Claude is trained using a constitutional approach that is more transparent, interpretable, and aligned with human values (De Freitas, 2025).

When developing a response to a spillover crisis involving GenAI, an effective differentiating strategy will typically involve a discussion around proprietary algorithms, safety measures, and human oversight (Prahl & Goh, 2021). These differentiating factors can be incorporated in an organization's response to highlight differences between the organization directly impacted by the crisis, and others adversely impacted by a spillover effect (Chang & Rim, 2024; De Feitas, 2025). In Table 1, we list examples of differentiation strategies that can be used with the different types of GenAI-related crises with spillover risks.

The importance of differentiation cannot be overstated when it comes to mitigating GenAI-related spillover risks. As discussed in Sections 1 through 3, spillover occurs because organizations are perceived to share technological infrastructures, ethical blind spots, or operational similarities. Therefore, differentiation for preventing, mitigating, and responding to spillover crises serves as a communicative tool to weaken both accessibility and diagnosticity in the public imagination (Feldman & Lynch, 1988; Roehm & Tybout, 2006). By clearly articulating how one's system, governance structures, or human oversight differs, companies can reframe their positioning in ways that reduce the perceived similarity to the organization involved in the GenAI-related crisis.

A good example involves Clearview AI, which experienced a privacy breach back in February 2020. Clearview is a facial recognition company with a database of billions of photos scraped from social media and the web. In response to the crisis, several companies issued denials, including the Bank of America: "We're not a client of Clearview," a Bank of America spokesperson said. "We haven't been a client, we didn't stop being a client, and we never were a client." (Mac et al, 2020). This is an example of how a company can differentiate itself by emphasizing that it does not use an AI system involved in a crisis.

When developing a differentiation strategy, it is important to ensure that it is crisis-type specific, corresponding directly to the five categories of GenAI-related crises identified in Table 1. For authenticity and integrity crises, differentiation requires proactive transparency. Organizations should emphasize early disclosure of GenAI use and clear labeling to demonstrate that they do not engage in deceptive practices (Deptula et al., 2025). For labor displacement crises, firms should highlight how GenAI is used to augment rather than replace human workers, aligning with broader narratives of employee empowerment and inclusivity (Chen et al., 2022; Chhibber et al., 2025). For technical failures, differentiation strategies should stress alternative systems, enhanced safety checks, and human-in-the-loop safeguards (Kaplan & Haenlein, 2020). In cases of data security and privacy crises, companies can highlight their proprietary protocols, stronger encryption, or selective partnerships with trusted providers to reduce diagnosticity (Prahl & Goh, 2021). Finally, for discrimination and bias crises, differentiation should focus on diverse training datasets, continuous auditing, and human oversight that ensures fairness in outcomes (Longoni et al., 2022).

The response strategies illustrated in Table 1 are examples of key points that should be communicated during spillover crises in the age of GenAI. However, simply claiming differentiation is not enough. Instead, companies must provide evidence, for example, in the form of technical documentation or third-party endorsements. This evidence-based communication contributes to reinforcing credibility (Coombs, 2007) and helps stakeholders distinguish between firms in ways that reduce the likelihood of guilt by association effects (Laufer & Wang, 2018). In particular, crisis communication must shift from generic assurances to tailored narratives that speak directly to stakeholder concerns tied to each crisis type (Laufer & Wang, 2018; Wang & Laufer, 2024).

[Insert Table 1 About Here]

Another point worth mentioning is that differentiation should not only be reactive but also anticipatory. As highlighted in earlier sections, diagnosticity is heightened when stakeholders perceive systemic flaws (Chang & Rim, 2024). By engaging in proactive disclosure and participating in self-regulatory initiatives, companies can build reputational buffers before a crisis occurs. For example, sector-wide commitments to transparency or fairness can reduce the diagnosticity of any single organization's failure, thus lowering the chances of spillover. This aligns with Barnett and King's (2008) insight that collective self-regulation can make reputational boundaries between organizations more visible, acting as "good fences" against crisis contagion.

In addition, differentiation should be understood as a dynamic, ongoing process rather than a one-off response. This is aligned with the "dynamic process" addressed by the crisis READINESS framework[2] (Jin et al., 2024; Jin et al., 2025; Voges et al., 2024). As stakeholder expectations evolve and as GenAI tools permeate more industries, companies must continuously adapt their communicative positioning. This involves monitoring social media narratives, engaging with watchdog groups, and remaining sensitive to emerging concerns about, for example, authenticity, integrity, privacy, and fairness (Holmström, 2022). Differentiation, then, is as much about sustained dialogue with stakeholders as it is about technological safeguards.

To conclude, managing GenAI spillover crises requires organizations to operationalize differentiation in ways that directly correspond to the five GenAI-induced crisis types. Effective communication must emphasize both preventive measures and reactive strategies, supported by credible evidence and continuous stakeholder engagement. An effective response can reassure stakeholders that the spillover crisis is not related to the organization and help prevent negative consequences such as reputational damage, negative word-of-mouth, or a decline in sales. By integrating differentiation into their broader crisis communication frameworks, companies can prevent guilt by association and preserve stakeholder trust in the age of GenAI.

[2] The READINESS framework (Jin et al., 2024; Jin et al., 2025) defines READINESS as a multidimensional construct that goes beyond traditional notions of preparedness or resilience. It comprises three interrelated dimensions: (1) multilevel efficacy, which includes self-efficacy at the individual level, collective efficacy at the team level, and organizational efficacy at the systemic level; (2) mindset, which emphasizes emotional leadership, mental adaptability, and a proactive orientation toward risks and crises; and (3) dynamic process, which views READINESS as an ongoing, adaptive process of learning and responding within complex and evolving crisis environments.

References

Barnett, M. L., & King, A. A. (2008). Good fences make good neighbors: A longitudinal analysis of an industry self-regulatory institution. *Academy of Management Journal, 51*(6), 1150–1170.

Bowen, S. A. (2024). "If it can be done, it will be done:" AI ethical standards and a dual role for public relations. *Public Relations Review, 50*(5), Article 102513.

Cardwell, H. (2023, June 6). Government ministry blocks AI technology from staff use. *RNZ News*. Available at https://www.rnz.co.nz/news/political/491407/government-ministry-blocks-ai-technology-from-staff-use

Chang, B., & Rim, H. (2024). Managing spillover: Response strategies to another charity's crisis. *Public Relations Review, 50*(3), Article 102413.

Chen, N., Li, Z., & Tang, B. (2022). Can digital skill protect against job displacement risk caused by artificial intelligence? Empirical evidence from 701 detailed occupations. *PLoS One, 17*(11), Article e0277280.

Chhibber, S., Rajkumar, S. R., & Dassanayake, S. (2025). Will artificial intelligence reshape the global workforce by 2030? A cross-sectoral analysis of job displacement and transformation. *Blockchain, Artificial Intelligence, and Future Research, 1*(1), 35–51.

Coombs, W. T. (2007). Attribution theory as a guide for post-crisis communication research. *Public Relations Review, 33*(2), 135–139.

Dastin, J. (2018, October 11). Insight - Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*. Available at https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG

De Freitas, J. (2025). Don't let an AI failure harm your brand. *Harvard Business Review*. Available at https://hbr.org/2025/07/dont-let-an-ai-failure-harm-your-brand?ab=HP-hero-latest-3

Deptula, A., Hunter, P. T., & Johnson-Sheehan, R. (2025). Rhetorics of authenticity: Ethics, ethos, and artificial intelligence. *Journal of Business and Technical Communication, 39*(1), 51–74.

Drayton, N. (2025, August 25). FTC sues to stop Air AI from using deceptive claims about business growth, earnings potential, and refund guarantees to bilk millions from small businesses. *Federal Trade Commission*. Available at https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-sues-stop-air-ai-using-deceptive-claims-about-business-growth-earnings-potential-refund

Feldman, J. M., & Lynch, J. G. (1988). Self-generated validity and other effects of measurement on belief, attitude, intention, and behavior. *Journal of Applied Psychology, 73*(3), 421–435.

Greene, J. (2024, August 2). Who's walking the runway: Fashion models or AI? *Global Legal Post*. Available at https://www.globallegalpost.com/news/whos-walking-the-runway-fashion-models-or-ai-198419621

Holmström, J. (2022). From AI to digital transformation: The AI readiness framework. *Business Horizons, 65*(3), 329–339.

Huang, Z. (2024, January 11). Chengdu charity under scrutiny for using AI-generated images on donation page. *China Daily*. Available at https://global.chinadaily.com.cn/a/202401/11/WS659fe55aa3105f21a507bd8b.html

Jin, Y., Coombs, W. T., Wang, Y., van der Meer, T. G., & Shivers, B. N. (2024). "READINESS": A keystone concept beyond organizational crisis preparedness and resilience. *Journal of Contingencies and Crisis Management, 32*(1), Article e12546.

Jin, Y., Shivers, B. N., Wang, Y., Coombs, W. T., & van der Meer, T. G. (2025). READINESS as a new framework for crisis management: Academic-industry integrated expert insights from practitioners and scholars. *Journal of Communication Management, 29*(1), 1–16.

Johnson, J. (2025, September 11). Coalition challenges OpenAI's nonprofit governance. *NPO*. Available at https://nonprofitquarterly.org/coalition-challenges-openais-nonprofit-governance/

Kaplan, A., & Haenlein, M. (2020). Rulers of the world, unite! The challenges and opportunities of artificial intelligence. *Business Horizons, 63*(1), 37–50.

Kunz, W. H., & Wirtz, J. (2024). Corporate digital responsibility (CDR) in the age of AI: Implications for interactive marketing. *Journal of Research in Interactive Marketing, 18*(1), 31–37.

Laufer, D., & Wang, Y. (2018). Guilty by association: The risk of crisis contagion. *Business Horizons, 61*(2), 173–179.

Laufer, D., & Wang, Y. (2024). Editorial: Special issue on the spillover effect of crises. *Public Relations Review, 50*(3), Article 102467.

Longoni, C., Cian, L., & Kyung, E. J. (2022). Algorithmic transference: People overgeneralize failures of AI in the government. *Journal of Marketing Research, 60*(1), 170–188.

Mac, R., Haskin, C., & McDonalds, L. (2020, February 28). Clearview's facial recognition app has been used by the Justice Department, ICE, Macy's, Walmart, and the NBA. *Buzzfeed News*. Available at https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement

Maher, A., & Singhapakdi, A. (2017). The effect of the moral failure of a foreign brand on competing brands. *European Journal of Marketing, 51*(5/6), 903–922.

Prahl, A., & Goh, W. W. P. (2021). Rogue machines and crisis communication: When AI fails, how do companies publicly respond? *Public Relations Review, 47*(4), Article 102077.

Ray, S. (2023, May 2). Samsung bans ChatGPT among employees after sensitive code leak. *Forbes*. Available at https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/

Roehm, M. L., & Tybout, A. M. (2006). When will a brand scandal spill over, and how should competitors respond? *Journal of Marketing Research, 43*(3), 366–373.

Salam, E. (2023, November 28). Sports Illustrated accused of publishing articles written by AI. *The Guardian*. Available at https://www.theguardian.com/media/2023/nov/28/sports-illustrated-ai-writers?

Savage, C. (2024, April 15). AI-generated models could bring more diversity to the fashion industry — or leave it with less. *AP News*. Available at https://apnews.com/article/ai-fashion-model-digital-diversity-aaa489111bd8e793aa6e5a531dc7ade2

Staton, B. (2023, April 3). Universities express doubt over tool to detect AI-powered plagiarism. *Financial Times*. Available at https://www.ft.com/content/d872d65d-dfd0-40b3-8db9-a17fea20c60c?sharetype=gift

Sweney, M. (2023, May 18). BT to axe up to 55,000 jobs by 2030 as it pushes into AI. *The Guardian*. Available at https://www.theguardian.com/business/2023/may/18/bt-cut-jobs-telecoms-group-workforce

Voges, T. S., Jin, Y., Buckley, C., Eaddy, L. L., & Lu, X. (2024). A new framework for managing "crisis spillover" as a type of sticky crisis: Initial insights from a crisis communication expert panel. *Public Relations Review, 50*(1), Article 102424.

Wang, Y., & Laufer, D. (2024). Crisis spillover effect: A review of the literature and an agenda for future research. *Public Relations Review, 50*(3), Article 102411.

West, D. (2023, March 23*).* Comparing Google Bard with OpenAI's ChatGPT on political bias, facts, and morality. *Brookings*. Available at https://www.brookings.edu/articles/comparing-google-bard-with-openais-chatgpt-on-political-bias-facts-and-morality/

Wiessner, D. (2024, February 21). Workday accused of facilitating widespread bias in novel AI lawsuit. *Reuters*. Available at https://www.reuters.com/legal/transactional/workday-accused-facilitating-widespread-bias-novel-ai-lawsuit-2024-02-21

Zampano, G. (2024, December 20). Italy's privacy watchdog fines OpenAI for ChatGPT's violations in collecting users' personal data. *AP News*. Available at https://apnews.com/article/italy-privacy-authority-openai-chatgpt-fine-6760575ae7a29a1dd22cc666f49e605f

Figure 1. The severity of crisis spillover risks

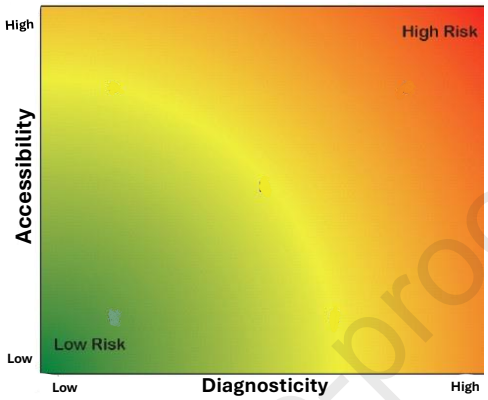

Table 1. Types of GenAI-related crises with spillover risks and response strategies

Crisis Types	Description	Examples	Strategies for avoiding this type of spillover crisis	Strategies for mitigating the negative consequences of this type of spillover crisis	Strategies for responding to this type of spillover crisis
Authenticity/ Integrity	Related to content trustworthiness and the erosion of credibility when using GenAI	*Sports Illustrated* was exposed for using fake author profiles for GenAI-generated articles, prompting sector-wide scrutiny of editorial authenticity in journalism	Avoidance requires clear disclosure of GenAI use and rigorous fact-checking to protect content credibility.	Mitigation depends on rapid audits and reinforcing human editorial oversight to restore confidence.	Response should distance the organization from unethical practices associated with the use of AI, such as the lack of disclosure, and emphasise the transparency around the use of AI by the organization in its operations to its stakeholders.
Labor Displacement	Employment risk associated with the use of GenAI	*Levi Strauss*' use of GenAI-generated models caused a public backlash about labor displacement, and it also raised concerns about job losses at other fashion brands as well	Avoidance requires upfront communication about workforce transformation and investment in reskilling.	Mitigation involves engaging employees and highlighting how AI complements rather than replaces human work.	Response should frame the incident as specific to the focal firm, deny parallels with its own employment policies, and emphasize that AI assists employees with productivity,

					but does not replace them.
Technical Failure	Highlights how technical failure in one company can spillover to other companies in the industry. This crisis type is related to concerns about the perceived reliability of GenAI tools	A self-driving car failure (operated by *Cruise,* a robotaxi subsidiary of *General Motors)* that injured a pedestrian led to broader distrust in autonomous vehicle safety	Avoidance rests on rigorous testing, external certification, and cautious rollouts before full deployment.	Mitigation requires immediate suspension of flawed systems, transparent reporting, and compensation for those affected.	Response should emphasise that the AI-related technical issue is unique to the affected company, and describe the different technologies or processes that it uses, in order to differentiate itself from the company experiencing the crisis.
Data Security & Privacy Concerns	Related to concerns over the use of data that is provided by organisations when using GenAI	New Zealand's government ministry banned staff use of GenAI tools due to data leak concerns, fueling broader scrutiny of GenAI adoption in public administration	Avoidance relies on privacy-by-design practices and clear rules for data handling.	Mitigation includes quickly updating protocols, publishing transparency reports, and seeking expert validation.	Response should distance the firm by clarifying it does not use the same AI tools or practices, deny exposure to the same vulnerabilities, and highlight strict proprietary safeguards.
Discrimination & Bias	Reflects systemic bias and structural inequality concerns in HR practices, extending beyond the	*Amazon*'s GenAI tool penalized female candidates and *Workday* was sued for GenAI-based hiring	Avoidance requires fairness testing, diverse training data, and ethical oversight during system design and use.	Mitigation can be achieved through corrective model adjustments and	Response should explicitly reject association with discriminatory practices and

	organizations directly involved when using GenAI	discrimination, raising systemic concerns about bias across the employment tech sector		inclusive stakeholder dialogue.	highlight distinct fairness protocols that set the firm apart. For example, emphasizing training AI tools on different data sets that are more representative of the population when compared with the company experiencing the crisis.