April 2017

McKinsey
Quarterly

Are you prepared for a corporate crisis?

No one can predict when disaster will strike—but knowing what to expect if it does will buy precious time.

by Sanjay Kalavar and Mihir Mysore

Imagine yourself as a top executive in a company hit by a major crisis within the last 72 hours. First, and most importantly, there may have been serious damage to the community in which you operate. Your customers may have suffered, people's livelihoods destroyed. The environment may be irretrievably damaged. Some of your employees and contractors may be injured, or worse. Your investors will be livid, and the board looking to assign blame. By the end of the first week, chances are your organization will be facing dozens of lawsuits, some set to become class actions over time.

Very likely, at this early stage, you will realize that verifiable facts are few and far between. Opinions and rumors abound. You will have little or no idea of the extent of any physical or financial damage or the extent to which the organization was complicit in the event. You don't even know which of your top team members you can count on. Some of them may be implicated; others may be operationally inexperienced, unfamiliar with the political realities, or temperamentally unsuited to the new situation—filled with good intentions but uncertain what role to play.

The crisis will be manna from heaven for your organization's natural antagonists, who will seek to take advantage of your misfortune. Competitors will try to lure customers and poach employees. Activist investors may plot a takeover. Hackers may target your systems. The media will dig up every past error the company may have made.

Much of the anger, by the way, is directed at you. And it's personal. Parody Twitter accounts may appear in your name, trashing your reputation. Your family may be targeted online. Reporters may be camping outside your home at odd hours of the day and night.

In the middle of all this chaos, what exactly do you do? Do you hold a press conference? If so, what do you say when you have so few facts? Do you admit wrongdoing, or do you say that what happened is not the fault of the company? Do you point to the cap on your legal liability, or do you promise to make everything right, no matter the cost? What do you tell regulators that are themselves under pressure, and demanding explanations?

The issues just described are not hypothetical. They are all real examples of experiences that organizational leaders we know have faced in multiple crises in recent years. What's really troubling is that these experiences are now far more frequent, and far more devastating, than they have been in the past.

Every crisis has its own unique character, rooted in specific organizational, regulatory, legal, and business realities. But after helping around 150 companies cope with a range of corporate disasters, we have seen some clear patterns. These can teach companies some simple best practices they can follow to prepare for a better response, in case the worst happens.

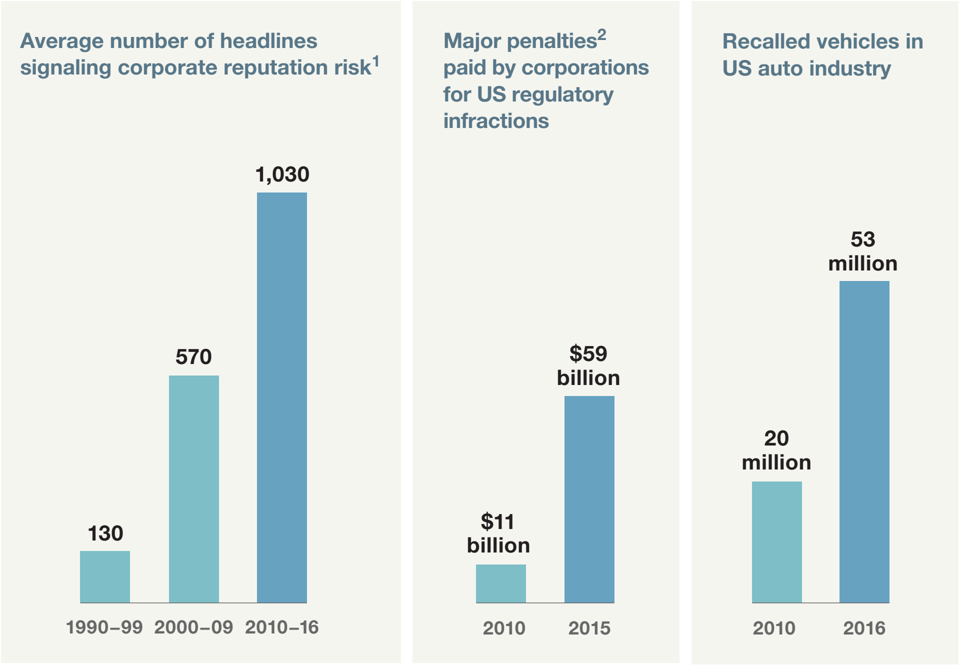
THE THREAT IS GROWING

Many incidents inside companies never hit the headlines, but recent evidence suggests that more are turning into full-blown corporate crises (exhibit). The total amount paid out by corporations on account of US regulatory infractions has grown by over five times, to almost $60 billion per year, from 2010 to 2015. Globally, this number is in excess of $100 billion. Between 2010 and 2017, headlines with the word "crisis" and the name of one of the top 100 companies as listed by Forbes appeared 80 percent more often than in the previous decade.[1] Most industries have had their casualties. For instance, the US auto industry recalled a total of around 53 million vehicles in 2016, up from about 20 million in 2010, while the US Food and

[1] Factiva; McKinsey Crisis Response analysis; top 100 based on the 2015 Forbes Global 2000 list.

Exhibit

Many company incidents remain hidden—but recent evidence suggests that more are turning into full-blown corporate crises.



[1] Reflects headlines with word "crisis" and name of one of top 100 companies in 2015 Forbes Global 2000 list.
[2] Major penalties defined as those exceeding $20 million.

Source: Factiva; National Highway Traffic Safety Administration; www.goodjobsfirst.org/violation-tracker

Drug Administration sent out nearly 15,000 warning letters to noncompliant organizations in 2016, up from just north of 1,700 in 2011.

Why is this a bigger problem now than it has been in the past? First is the growing complexity of products and organizations. A new pickup truck today includes computer controls programmed with more than 150 million lines of computer code, while the average deepwater well is the height of seven Eiffel Towers. Goods travel thousands of miles and move through supply chains that comprise multiple intermediaries and multiple jurisdictions. A second reason for the significance of the problem is a higher level of stakeholder expectations. Customers, often in response to messages on social media, are more willing to sue or shun a company they believe is unethical. Governments are more willing to seek redress from companies they believe are breaking the law, and shareholder activism is on the rise. Third, the changing social contract is driving anxieties and mistrust in institutions, making irreversible knee-jerk reactions more likely. Finally, the raw speed of business operations—from rapid communications to shorter product-development timelines—makes crises more likely.

Understandably, companies spend more time trying to prevent crises than preparing for them. However, crisis readiness has become at least as important as risk management, takeover readiness, and vigilance over safety.

Underpreparedness has consequences and helps explain why companies engulfed by a large crisis initially underestimate the ultimate cost by five to ten times.[2] Senior executives are frequently shocked by how quickly a problem can turn from a minor nuisance into an event that consumes and defines the company for years to come.

FIVE PARALLEL PATHS TO RESOLUTION

In our experience, it helps to think of a crisis in terms of "primary threats" (the interrelated legal, technical, operational, and financial challenges that form the core of the crisis) and "secondary threats" (reactions by key stakeholders to primary threats). Ultimately, the organization will not begin its recovery until the primary threats are addressed, but addressing the secondary threats early on will help the organization buy time.

When a crisis hits (or is about to hit), one of the first actions should be to create a cross-functional team to construct a detailed scenario of the main primary and secondary threats, allowing the company to form early judgments about which path the crisis may travel. This helps the organization set out major decisions it needs to make quickly and is the first step toward wresting back control—improving the headlines of tomorrow, rather than merely reacting to the headlines of today.

While it is rare to get everything right at this stage, it is equally rare to get most of the second-order effects wrong. People are innately overoptimistic, of course, as we know from work on cognitive biases, but even being half right about how things will unfold is valuable at this early stage. It will provide a strong basis for tackling the five broad issues we see as critical to the outcome of a crisis: controlling the organization, stabilizing stakeholders, resolving the immediate primary threats, repairing the root causes of the crisis, and

[2] McKinsey Crisis Response analysis: ratio of initial company and analyst expectations in multiple crises (as measured by initial drop in market cap) to final cost.

restoring the organization over time. While all five need to be started early, they will likely require different levels of emphasis at different stages.

Control the organization

Normal rules for how the organization operates get torn up quickly in a crisis. Informal networks founded on trust and the calling in of favors can dominate over formal organizational reporting structures. Those previously opposed to the status quo can quickly become vocal, sparking a turf war and delaying action. Some key executives may themselves be implicated and unable to lead the response. Managers may start executing an uncoordinated set of actions with the best of intentions but incomplete or inaccurate information. No longer able to build consensus, they end up with unwieldy organizational structures that have dozens of decision makers around a table, with the result that the effort becomes dispersed and disconnected.

All this explains why an effective crisis team is central to mounting a satisfactory response. The best crisis organizations are relatively small, with light approval processes, a full-time senior leader, and very high levels of funding and decision-making authority. The team should be able to make and implement decisions within hours rather than days, draw a wall of confidentiality around the people who are responding, and protect those not involved from distraction in their day-to-day activities.

A common error is to choose an external expert as leader of the company's crisis response. External hires typically struggle to motivate and organize the company in a crisis situation. The right leader usually will be internal, well known, and well regarded by the C-suite; will have served in an operational capacity within the industry; and will enjoy strong informal networks at multiple levels in the company. He or she should possess a strong set of values, have a resilient temperament, and demonstrate independence of thought to gain credibility and trust both internally and externally.

The ideal crisis organization includes a set of small, cross-functional teams, typically covering planning and intelligence gathering, stakeholder stabilization, technical or operational resolution, recovery, investigation, and governance.

Stabilize stakeholders

In the first phase of a crisis, it's rare for technical, legal, or operational issues to be resolved. At this stage, the most pressing concern will likely be to reduce the anger and extreme reactions of some stakeholders while buying time for the legal and technical resolution teams to complete their work.

For instance, an emergency financial package may be necessary to ease pressure from suppliers, business partners, or customers. Goodwill payments to consumers may be the only way to stop them from defecting to other brands. Business partners might require a financial injection or operational support to remain motivated or even viable. It may be necessary to respond urgently to the concerns of regulators.

It's tempting and sometimes desirable to make big moves, but it is tough to design interventions that yield a tangible positive outcome, from either a business or a legal standpoint. What usually works is to define total exposure and milestones stakeholder by stakeholder, then design specific interventions that reduce the exposure.

Resolve the central technical and operational challenges

Many crises (vaccines in pandemics, oil wells during blowouts, recalls in advanced industries) have a technical or operational challenge at their core. But the magnitude, scope, and facts behind these issues are rarely clear when a crisis erupts. At a time of intense pressure, therefore, the organization will enter a period of discovery that urgently needs to be completed. Frequently, however, companies underestimate how long the discovery process and its resolution will take.

Companies' initial solutions simply may not work. One manufacturer had to reset several self-imposed deadlines for resolving the technical issue it faced, significantly affecting its ability to negotiate. Another company in a high-hazard environment made multiple attempts to correct a process-safety issue, all of which failed very publicly and damaged its credibility.

It's best, if possible, to avoid overpromising on timelines and instead to allow the technical or operational team to "slow down in order to speed up." This means giving the team enough time and space to assess the magnitude of the problem, define potential solutions, and test them systematically.

Another frequent problem is that the technical solution, mostly due to its complexity, ends up becoming a black box. To avoid this, technical and operational war rooms should have an appropriate level of peer review and a "challenge culture" that maintains checks and balances without bureaucratic hurdles.

Repair the root causes

The root causes of major corporate crises are seldom technical; more often, they involve people issues (culture, decision rights, and capabilities, for example), processes (risk governance, performance management, and standards setting), and systems and tools (maintenance procedures). They may span the organization, affecting hundreds or even thousands of frontline leaders, workers, and decision makers. Tackling these is not made any easier by the likely circumstances at the time: retrenchment, cost cutting, attrition of top talent, and strategy reformulation.

For all these reasons and more, repairing the root cause of any crisis is usually a multiyear exercise, sometimes requiring large changes to the fabric of an organization. It's important to signal seriousness of intent early on, while setting up the large-scale transformation program that may be necessary to restore the company to full health. Hiring fresh and objective talent onto the board is one tried and tested approach. Other initiatives we've seen work include the creation of a powerful new oversight capability, the redesign of core risk processes, increased powers for the risk-management function, changes to the company's ongoing organizational structures, and work to foster a new culture and mind-set around risk mitigation.

Restore the organization

Some companies spend years of top-management time on a crisis, only to discover that when they emerge, they have lost their competitiveness. A large part of why this happens is that they wait until the dust has settled before turning their attention to the next strategic foothold and refreshing their value proposition. By this stage, it is usually too late. The seeds for a full recovery need to be sown as early as possible, even immediately after initial stabilization. This allows the organization to consider and evaluate possible big moves that will enable future recovery, and to ensure it has the resources and talent to capitalize on them.

BE PREPARED

Much of the training top executives receive around crisis management is little more than training in crisis communications—only one part of the broader crisis-response picture. The sidebar (see "Are you prepared for the worst?") lays out the sort of questions about preparedness that companies should be asking themselves.

Companies—and boards—should consider clearly defining the main "black swan" threats that may hit them, by conducting regular and thorough risk-

ARE YOU PREPARED FOR THE WORST?

TWENTY-FIVE QUESTIONS EXECUTIVES SHOULD ASK THEMSELVES NOW

UNDERSTANDING THREATS

- What are the organization’s top ten risks and, relative to these, what are the top five “black swan” threats that could destabilize the organization?
- For each black-swan threat, how might the crisis evolve, including second-order effects by stakeholders and assessments of maximum exposure?

ORGANIZATION AND LEADERSHIP

- What will the crisis organization look like for each threat (in particular, is there a crisis-response leader with the right temperament, values, experience, and reputation), and when will that organization be activated?
- What will be your organization’s governing values and guiding principles if any of the black swans hit?
- Have you defined the blueprint for a central crisis nerve center staffed by top executives, with division of roles?
- Do you have a crisis governance structure that involves the board, drives decision making, and isolates the rest of the business?
- Do you have a succession plan in case some of your mission-critical leaders need to step down because of the crisis?

STAKEHOLDER STABILIZATION

- Have you defined key stakeholders, including competitors and influencers, and tested how they might act in a crisis?
- Have you invested in understanding and establishing relationships with regulators and government stakeholders?
- Do you have a plan to protect employees and reduce attrition of your most talented employees?
- Have you established the portfolio of actions to stabilize stakeholders in the event of each scenario, beyond public relations?

OPERATIONAL AND TECHNICAL

- Which critical operations can keep going, and which ones may need to slow or stop?
- Is there a blueprint for an operational or technical war room staffed with the right team and adequate peer review?
- Have you defined ways to monitor and reduce cyberthreats, including dark web scans, during a crisis?

INVESTIGATION AND GOVERNANCE

- How will you scope an investigation, and what level of transparency might you need to provide?
- Do you have a set of options for large governance changes you may need to make after a crisis?

MARKETING, BRAND, AND COMMUNICATIONS

- Have you established a basic communications process, tools, roles, and plan to drive key messages with stakeholders?
- Have you thought how to protect your brand during the crisis and help it recover afterward?

FINANCIAL AND LIQUIDITY

- Are there financial protocols to provide crisis funding, protect liquidity, and maintain the business?
- Have you defined the broad scope of root-cause investigations and how they will be governed?

LEGAL, THIRD PARTY, AND OTHER

- Does the crisis team have a working knowledge of relevant legal provisions, case law, and protocols?
- Have you pre-identified battle-tested third parties, such as law firms, crisis communications firms, coordination, and business decision making?
- Do you have a sense, based on case law, what the overall legal pathways may be to resolve the black-swan event?
- Have you identified critical suppliers and considered how existing terms and conditions will affect you adversely in a crisis?

READINESS

- Have you rehearsed and critiqued all of your biggest crisis scenarios at least once in the past 12 months and implemented improvements to processes or other changes arising from these exercises?

identification exercises and by examining large crises in other industries as well as in their own. Once they do this, they should lay out, for each threat, what the trigger may be and how a hypothetical scenario for a crisis might unfold, based on patterns of previous crises. This allows the company to examine critically areas of weakness across the organization, and to consider what actions could offset them. For instance, should the company consider revisiting terms and conditions for key suppliers and building in a "cooling period," rather than being forced to change the terms of accounts receivable in the heat of the moment? What other measures would provide short-term liquidity and steady the ship financially? Should the company invest in an activist-investor teardown exercise to assess key vulnerabilities that may surface in the midst of a crisis?

Once such an assessment is complete, the company should train key managers at multiple levels on what to expect and enable them to feel the pressures and emotions in a simulated environment. Doing this repeatedly and in a richer way each time will significantly improve the company's response capabilities in a real crisis situation, even though the crisis may not be precisely the one for which managers have been trained. They will also be valuable learning exercises in their own right.

Risk prevention remains a critical part of a company's defense against corporate disaster, but it is no longer enough. The realities of doing business today have become more complex, and the odds of having to confront a crisis are greater than ever. Armed with the lessons of the past, companies can prepare in advance and stand ready to mount a robust response if the worst happens.

Sanjay Kalavar is a senior partner in McKinsey's Houston office, where **Mihir Mysore** is a partner.

The authors wish to thank Manu Balakrishnan, Malik Ben-Yousef, Parmeet Grover, Thomas Seitz, and Chiranjeev Singh for their contributions to this article.