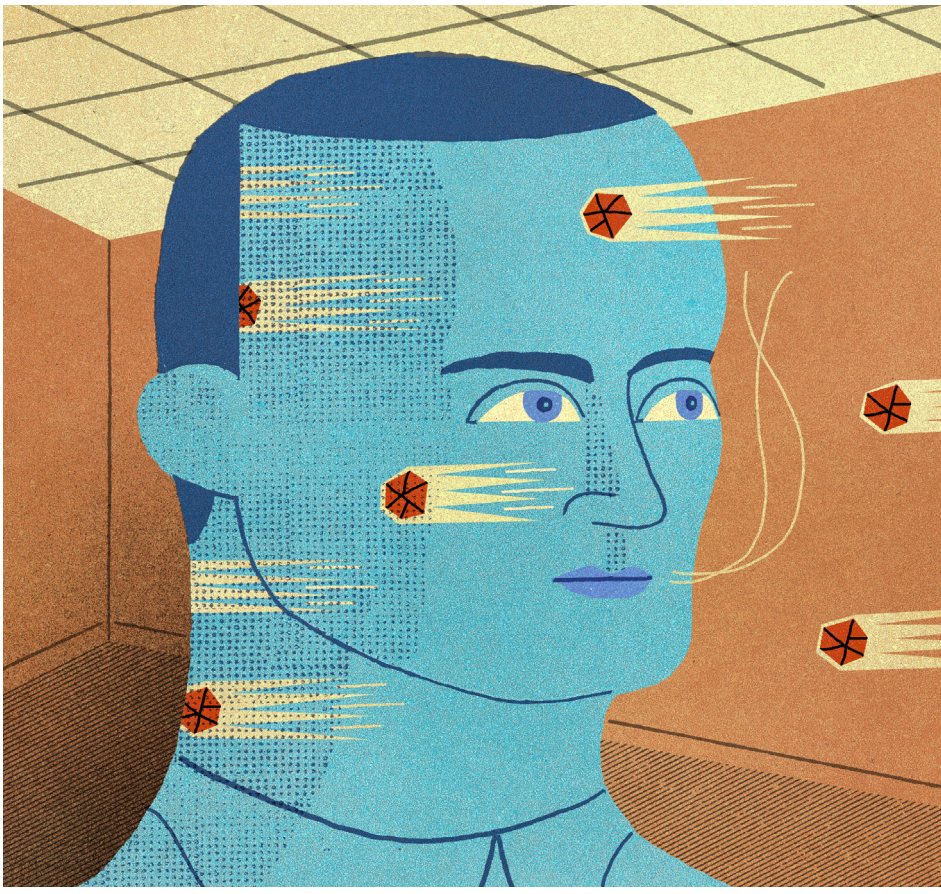


Crisis Psychology

In a time of mounting stress, the expectations on decision makers weigh heavily. Drawing on Brunswick's experience, **MARINA BIDOLI** and **PAULA FIORINI** walk us through the pressures of a crisis war room.

In a crisis, when uncertainty is rising and stakeholder scrutiny is intensifying, decisions that normally take weeks are compressed into hours. There is a persistent sense of jeopardy and incomplete information, yet ultimately decisions are necessary.

A serious misstep can carry personal and organizational consequences. Typically, too, the cost of waiting can exceed the cost of an imperfect decision. "Speed is better than being 100% right," as one Brunswick client put it. The psychological pressure is intense.

Anyone who has spent time in a crisis war room will recognize the pattern: People move rapidly between shock and disbelief, anger and blame, fear and isolation, loss of control and exhaustion—sometimes cycling through these emotions several times in a single day. Acceptance can take months or even years as events evolve, new facts reopen old questions and stakeholder reactions make a supposedly resolved issue suddenly feel unresolved. What first looked like an operational failure can, days later, become a cultural or reputational one. There is no straight line from shock to acceptance to recovery.

Our recent international Leadership Stress Index survey shows that not only is the frequency of such crises escalating, but stress levels now are greater even than during COVID. One respondent told us, "During the pandemic there was a clear enemy, a shared enemy. Now it's coming from all directions."

That takes a toll on C-suite psychology that can hamper decision making. Just when a situation would demand clarity and calm, "We were fueled by our emotions," one CEO told us about a moment in particular. It's a sentiment we hear repeatedly in hundreds of conversations with senior leaders navigating periods of intense pressure and uncertainty. Ultimately, any decision rests with the CEO or chair, but the thinking behind it does not have to.

This is where board members and external advisors can come into play. Not to manufacture reassurance, but to provide objectivity; to identify plausible scenarios, anticipate stakeholder reactions, separate genuine threats from political and media noise, help leadership distinguish an existential problem from an extraordinarily painful but manageable one, and, ultimately, to help guide leadership to do the right thing.

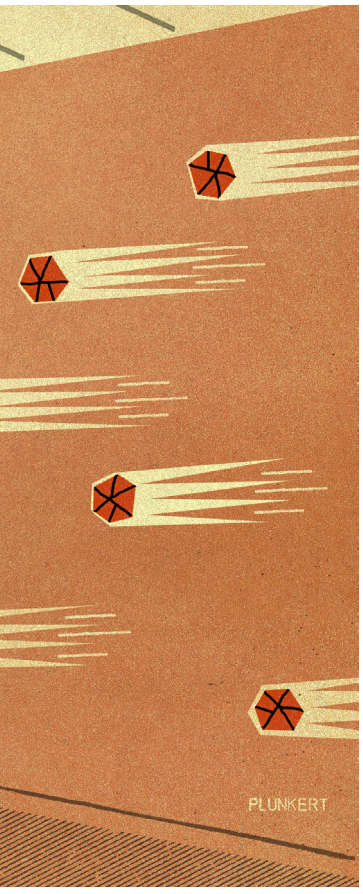
The need in these moments is to talk to someone who has weathered similar crises before, and who is less likely to be caught by the emotional undertow. A typical leader will see at most a few such crises in a long career; a firm like Brunswick has seen thousands. No two are exactly alike, but lessons drawn can apply across the board.

FLYING BLIND

Consider a cyberattack on an offshore subsidiary of a global, NYSE-listed group. The local CEO suddenly lost control of his operations, with the attackers advancing on the one hand and US headquarters deeply involved on the other. Clients were clearly at risk. Regulators were circling and the potential for catastrophic fines was being discussed.

Then, it turned personal. The threat actor was leaking information, doing media interviews and making physical threats serious enough for the CEO to increase security for himself and his family. The CEO was simultaneously trying to protect customers and employees, answer headquarters, deal with regulators and the media, and consider which new routes his family should take to work and school.

ILLUSTRATION: DAVID PLUNKERT



"WHEN EVENTS UNFOLD AT TWO IN THE MORNING, YOUR MOST VALUABLE ASSET IS HAVING THE RIGHT PEOPLE, IN THE RIGHT PLACE, ALREADY ALIGNED AND READY TO ACT."

Invariably, no exercise in preparation foresaw circumstances this stark. No communications manual existed for this situation. Without help, a CEO and board can feel as though they're flying blind.

Our experiences at Brunswick have shown again and again that structure—which outside agitators are constantly trying to undermine—is an invaluable ally in these moments. Clear crisis protocols can reduce a sprawling situation into something manageable: Here is the decision. Here is who owns it. Here is what we know. Here is what we do not know. Here is when we need to revisit each question.

In this case, steadfast rigor won the day. It was a long haul, but the company and its leadership survived and went on to thrive. And four years after the breach became public, regulatory authorities were satisfied and the matter was closed without a fine.

THE KRAKEN

When crises involve political influence, public institutions and private interests, they can unfold on an extraordinary scale, dominating local and international news, crossing borders, institutions and stakeholder groups. Examples include South Africa's State Capture, Brazil's Lava Jato, Malaysia's 1MDB and Italy's Tangentopoli scandals. Across the world, organizations implicated in corruption probes have often found themselves confronting consequences far beyond the circumstances that first drew them in.

What initially appears as a question about an individual contract, client or relationship can become something much bigger: a question about governance, incentives and culture. What begins as a local issue can very quickly become a global reputational crisis that attracts international media attention. Why was this subsidiary generating so much revenue? What relationships were making that possible? Who were its clients and intermediaries? What did headquarters know, or what should it have known?

Inside the war rooms of global firms engulfed in such crises, late nights are spent piecing together incomplete and contradictory evidence; compliance and legal teams dispatched from headquarters show up to establish what happened; there's suspicion between colleagues, defensiveness and uncertainty. There's fear.

As official investigations intensify the pressure, country heads lose their jobs, executives leave. As days become months and years, a siege mentality sets in, with exhaustion, shame and increasingly desperate questions: "When will this end?" And later, "Haven't we done enough to remediate?"

Operations across borders are needed to monitor and respond to media coverage, engage with regulators and governments, and manage relationships with stakeholders. When events unfold at two in the morning, your most valuable asset is having the right people, in the right place, already aligned and ready to act—this is an asset one client termed "zero friction." That requires planning with the right partners.

Yet survival depends mostly on that same combination of structure, perspective and execution that succeeded in the cyberattack example. In fact, its value becomes clearest when a crisis expands to include institutions, governments and society.

RECOVERY & AFTERMATH

Long before the resolution of a prolonged crisis, as the pieces of the immediate response fall into place, eyes already need to be shifting to the long term. The question, "How do we survive this?" becomes, "How do we want to be regarded five years from now?"

Too often, organizations assume that when the headlines fade, the crisis is over. Stakeholders rarely agree. The IT system is restored. The investigation is complete. The immediate threat has passed. But trust operates on a different timetable.

The work of British disaster-recovery expert Lucy Easthope offers a useful lens. In her book, *Come What May*, she describes a long, uneven recovery curve following catastrophe: After impact comes a heroic or "honeymoon" phase, when adrenaline is high, people pull together and attention and resources pour in.

Then comes the harder period of disillusionment and then "the slump." Attention moves elsewhere. Emergency machinery disperses. Exhaustion sets in just as the scale of the long, unglamorous work of recovery becomes clear. Only then does reconstruction begin, rarely in a straight line back to what came before.

Leadership shifts from survival to recovery, to the question of how to earn back trust and rebuild stronger. Resolving a cyberattack does not necessarily reassure customers that their data will be safe next time. Replacing an executive does not prove that the culture has changed. An apology does not demonstrate that lessons have been learned. Communication remains critical.

Ultimately, recovery has to be demonstrated through action.◆

MARINA BIDOLI is a Partner in Brunswick's Milan office and former head of the South African office.
PAULA FIORINI is a Director in London.