Teneo

# A conversation with Teneo Risk Senior Advisor Juliette Kayyem about her new book *The Devil Never Sleeps: Learning to Live in an Age of Disasters*

Teneo Insights / February 2022

**Juliette Kayyem**
Senior Advisor
juliette.kayyem@teneo.com

Teneo Risk recently sat down with Teneo Senior Advisor Juliette Kayyem, CEO of Grip Mobility and Senior Belfer Lecturer in International Security at Harvard's Kennedy School of Government, about her upcoming book, The Devil Never Sleeps, which discusses how leaders can prepare for and deal with the never-ending onslaught of disasters.

**Teneo:** Juliette, two years into the COVID-19 pandemic, and with Omicron variant cases believed to have peaked, we are all starting to feel like we are finally on the other side of this. However, as you note at the very beginning of your new book, disasters are not one-off, isolated events. Rather, they are the norm. As companies prepare to return to some degree of pre-pandemic normalcy while continuing to grapple with a myriad of pandemic-related and other challenges, how would you advise CEOs to think about how they should prepare for the next pandemic or other disaster?

**Juliette:** I will begin by saying that disaster is an inevitability. Despite the best efforts of any leader, regardless of whether they are in government or in the private sector, disasters will continue to be a perennial threat throughout and beyond the COVID-19 pandemic. Traditional crisis management seeks to avoid disaster and minimize the consequences upon its arrival. I argue that we need to stop being surprised. All leaders must structure their entities and agencies around the probability of some disaster, not the mere possibility, to better invest and nurture the capabilities to minimize the harm to follow.

Knowing that disaster will arrive necessitates preparation now, that is, that preparation is not for some distant future, related to the "later" box, but here, right now. Traditional crisis management divides the world into two moments: left and right of boom, before and after the disaster. The left-of-boom stage encapsulates the investments an entity makes to avoid this boom from happening, and those prevention and protection efforts to delay or avoid this ever-looming devil. Despite our best efforts, this "boom" will ultimately arrive, so we must focus on the right-of-boom activities; all those things we do to respond, to recover and to build more resilience again. I seek to illustrate how we can live more confidently in anticipation of that right-of-boom, fostering responses time and again.

This begins with acknowledging and structuring ourselves and organizations around the idea that at some point and time we will be on the right side of the boom. If, when the disaster ends, we move on because we believe the disruption was an aberration or surprise, we will not examine the deprivations that led to such horrible consequences in the first place. The devil will have won the round, and he will return all the sooner. My goal is to disabuse agencies, businesses and their leaders of the notion that there is a finish line, a misconception that ignores the potential to do better now.

**Teneo:** You have spent over 20 years managing complex policy initiatives and organizing government responses to major crises in both state and federal government. In your book, you note that for so many institutions, crisis or disaster management is seen solely as some combination of the three Gs: gates, guards, and guns. Once executive leadership has wrapped their heads around the fact that disaster is inevitable, and that they need to prepare for it, how would you advise they ideally go about this?

**Juliette:** The knowledge of disasters' inevitability requires executive leadership, especially CEOs and other C-Suite executives, to envision themselves as crisis managers. CEOs must incorporate a basic design feature into their organizations that embraces the idea that the worst-case scenario is possible again and again. And again. What then?

A CEO does not have to be an expert on the intricacies of tactical operations or planning but must ensure that those systems are fully nurtured and integrated. Corporate governance requires that all the pieces of governance, and all those moving parts from the security apparatus and reporting structure to board structure and membership, are unified. It is imperative that CEOs embrace what I call "unity of effort," corporate governance planning that ensures a collectiveness when the boom arrives. Far too often preparedness is distributed, often leaving security efforts vulnerable as systems are fragmented and disjointed. The "architecture of security" concept expresses the idea that for an organization to maximize safety and security planning, it must establish a governance structure that embraces all capacities. CEOs must take the lead in constructing a security architecture that includes all elements of response capabilities, overcoming the traditional and insufficient planning of the three Gs: gates, guards, and guns.

Firms must pivot to a method of sustainable protocols, incorporating security into an organization's apparatus not as an add-on, but as an integral part of the architecture of security. Response capabilities and security teams must be viewed as business enablers. The current tendency to build bad architecture, to set what should be a harmonious table as if everybody is only a party of one, is often exacerbated by the lack of focus at the top. Different C-leaders in security not only have different reporting structures and chains of command but are not granted voice in leadership or the board of directors. Additionally, few of these boards have a single individual from the security or cybersecurity realm, indicating that these individuals are not integral to the company's business model and denying their access to and influence over top corporate leaders. I can't reiterate enough that every leader must ensure that the architecture of their institution is aligned for unity of effort. As I write in my book, you don't want the physical security gal to be meeting the cyber response guy at the moment of impact.

**Teneo:** A challenge that you note to optimal, or even adequate, disaster preparedness is what you term the "sunk cost fallacy," which you frame as the "mere fact of that investment justifies continuing the same behavior regardless of whether that behavior is still warranted because the resources are committed." Can you elaborate on what you mean by this and how CEOs should instead be thinking about the investment required to continually reexamine and reevaluate their disaster preparedness/mitigation/management strategies?

**Juliette:** Safety and security systems are designed based on conditions that existed when they were built. Without compelling evidence of change, we often come to believe that those conditions are constant. If it worked in the past, and is working now, why shouldn't it continue to work? If a sophisticated cybersecurity network halted the last breach, why not the next? We now know this thinking is not only untrue, but dangerous. Fundamentals are always changing. If the threat was always the same, we would have long ago mastered disaster and crisis management. As I articulate in my book, preparation for the boom is never complete, especially when it can come any day, every day, a perennial threat that should inform constant reassessment.

I have too often seen organizations build sound preparedness measures only to let these measures linger in the face of constant and evolving threats. They felt as if they were done, as if disasters were random and rare. This thinking is likely explained by the sunk cost fallacy. In the field of economics, a sunk cost describes an investment that has already been made and can no longer be recovered. The fallacy arises when the mere fact of that investment justifies continuing the same behavior, regardless of whether that behavior is still warranted, because the resources are committed. We no longer consider whether the effort is still a good investment because we already committed time and money. The fallacy assumes that there is a single static investment that holds over time; but planning should not remain static. As organizational leaders, CEOs must rid themselves of this fallacy.

Sustained preparedness requires thinking of preparedness not as static, but as a moving target. There simply is no finish line. Prior investments may have been useful at a certain moment in time but are very rarely useful for the ever-present threat of the end of times. Previously established capabilities only represent a moment in time tied to that instance or threat and must be constantly revised to prepare for different disasters to come.

**Teneo:** One of the primary goals for organizational resilience that you identify is sustained preparedness, an ever-present awareness of an imminent unknown. How can organizations ensure that their planning can adapt with an eye to the future? Are there any specific methods that are imperative to incorporate into a company's crisis management and resilience program?

**Juliette:** The most effective way to ensure that the planning of today can adapt to the future is to continuously stress test the system. Stress tests, when enacted thoroughly, cannot be underestimated, adding purposeful variation to preparedness as it challenges any existing planning. Most importantly, these tests can expose where a response system has gaps or weaknesses. I think that this is where a notion called red teaming is very useful. In military war-gaming, there is an exercise called "red teaming," that is enacted to challenge plans, policies and assumptions by exposing oneself to an adversary that perpetually challenges conventional wisdom. The military sets up an opposing force, the red team, in a fictional conflict that serves as a test against the "defenders," the blue team, who are unaware of the red team's plans. The enemy may have new weapons, techniques and capabilities, and they are a purposeful, determined force. The exercise emulates battle in that both teams physically move in response to each other and that it forces the blue team to break from the expectations of the past in response to new threats. Operational issues are put under scrutiny, providing alternative analysis.

The exercise can be used outside of the military to significantly improve an organization's resilience. For example, work teams can bring in outsiders to meet and discuss different responses to an array of hypothetical scenarios. Planning and communicating about existing expectations can reveal flawed assumptions and help teams adapt. When an outside group, a red team, is brought in to propose various scenarios in a simulation that is constantly changing based on decisions made by the blue team, assumptions are immediately challenged, helping an institution determine the success of their response planning. Corporations with strong cybersecurity resilience often hire hackers, who they euphemistically call ethical hackers, to use all resources at their disposal to hack into the computer system. The goal is to see if the company can defend against such threats and mitigate any damage. These stress tests add purposeful variation to preparedness, revealing any insufficient planning.

**Teneo:** You note that left-of-boom awareness-risk assessments and intelligence reports are not often accompanied by mechanisms to gather and disseminate information as disaster unfolds. What is the importance of situational awareness and the collection/dissemination of information as disasters occur? What role should CEOs play in creating situational awareness capacity to assess real-time needs during crisis?

**Juliette:** When looking at disasters with the benefit of hindsight, the way in which they unfolded is already written. Events, times and places are rapidly reported on, analyzed, written about and understood. The failure to respond sufficiently in real time often looks negligent or misguided. However, in real time, as disasters are unraveling, what is in fact happening is not so easily known. Information and disinformation, data, rumors and suspicions all struggle for the spotlight in moments of distress. It is imperative that CEOs build up sufficient mechanisms for their organizations to gather information as a disaster unfolds that assist in driving a response, make that response more effective and minimize consequences.

We focus a great deal on "intelligence failures," the left-of-boom awareness (or lack thereof), but very little on how the crisis is unfolding and how to mitigate losses in real time. As CEOs lead their organizations to a model of sustainable preparedness-situational awareness, the way first responders document what is happening and necessary responses, as well as attempts to document what may happen next and what will be needed, will be essential for effective consequence management.

Situational awareness is not just about aligning capabilities with existing data and information but describing the methods and processes in place to assess what is happening as the damage unfolds, so that a leader can be best prepared to minimize consequences. For consequence minimization, various leaders within an organization require mechanisms to know what is happening so that resources can be utilized where needed and re-directed to where they may be needed in the future, tools incumbent on the CEO to provide. A simple and effective situational awareness document includes three parts: what is happening, what it means, and what may likely happen. As crisis does inevitably strike, leaders need to embrace two key needs in managing and limiting the impact: numbers and hope. CEOs must be ready for their organizations to use basic data to guide response and an empathic acknowledgement that what is happening now will get better.

The Devil Never Sleeps will be available in March 2022. To pre-order a copy, please visit: The Devil Never Sleeps | by Juliette Kayyem. To set up a meeting or consultation with Juliette and the Teneo Risk team, please email naureen.kabir@teneo.com.

Teneo®

## Teneo is the global CEO advisory firm.

Teneo is the global CEO advisory firm. Working exclusively with the CEOs and senior executives of the world's leading companies, Teneo provides strategic counsel across their full range of key objectives and issues.

Teneo's clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations. Integrating the disciplines of strategic communications, investor relations, restructuring, management consulting, physical & cyber risk, financial advisory, corporate governance advisory, ESG,  DE&I, political & policy risk, and talent advisory. Teneo solves for the most complex business challenges and opportunities.

**teneo.com**