Chapter 2

Crises: A Major Systems Problem

In the last chapter, we showed that Defense Mechanisms operate on at least two levels, the personal and the organizational. They also apply equally to institutions and thus to societies as a whole. Indeed, they relate to every aspect of our Being.

In this chapter, the levels and interactions become even more pronounced. Thus, every type of crisis not only applies to, but has direct counterparts at the personal, organizational, national, and international bearings of our existence. In brief, there is no such thing as single, self-contained, independent, and isolated crises. Every crisis is capable of being both the cause and the effect of every other. In fact, unless one is prepared to think and to act Systemically, every crisis is capable of setting off an uncontrolled chain reaction of additional crises, and in many cases, those that are even worse than the initial ones. For this reason, it's never sufficient to plan for individual crises in isolation. In fact, it's completely counterproductive. Thus, Systems Thinking is key. (For this reason, we give an in-depth treatment of Systems in Appendix 3.)

For instance, in 2015, the automaker, Volkswagen (VW), experienced a severe Public Relations Crisis when it came to light that the company had systematically lied about the true, unacceptable levels of pollutants emitted from its cars' engines. What began as a PR crisis soon became a major Financial Crisis. And, it quickly became an Ethical and Organizational Crisis when the company executives who had approved the practice were identified and publicly castigated. Indeed, the blame went all the way to the top showing that crises are rarely contained.

Mitroff and his colleagues have identified the following major categories and types of crises. Each contains a never-ending series of subtypes. For this reason, they are better thought of as different, ever-expanding "families of crises:"

- Product recalls/defective products
- Product/service tampering
- Employee sabotage/nefarious actors
- Fires/explosions/chemical spills

- Environmental disasters/climate change
- Significant drop in revenues/financial
- Natural Hazards
- Loss of confidential/sensitive information/privacy
- Terrorism
- Ethical breaches
- Technological

Notice that instead of the usual category “Natural Disasters,” the label “Natural Hazards” has been chosen deliberately. The reason is that all crises are “Human-Caused.” For it’s humans, not Mother Nature, who make the important decisions where to build houses and other structures and to what standards and building codes. In this way, all disasters bear the indelible imprint of humans and, in this sense, are “Human-Caused.” As a consequence, they are better labeled “Natural Hazards.” Humans are responsible for turning Hazards, such as Earthquakes due to Fracking, into Crises.

To show how each of the various types spans multiple levels and gives rise to a host of different crises, consider the important case of Technology.

2.1 Managing Technology

[Zuckerberg] is right that our democracy can survive a pandemic. It is unclear, however, if it can survive a platform optimized for conspiratorial thinking. Like industrial-age steel companies dumping poisonous waste into waterways, Facebook pumps paranoia and disinformation into the body politic, the toxic byproduct of its relentless drive for profit. We eventually cleaned up the waste. It’s an open question we can clean up after Facebook.¹

The Management of Technology is arguably one of the most important problems facing humankind.² Indeed, second only to Climate Change and the Global Pandemic due to the Coronavirus, it is arguably the most important of all.

For better and for worse, we are engaged in nothing less than the “complete, if not revolutionary, alteration/control” of the Human Body, Mind, Reality, Trust, and Truth itself. In short, for good and for bad, there is not a single aspect of our existence that Technology does not affect in an important way.

Thus, on the one hand, Social Media have allowed us to communicate widely and instantly with scores of “new friends,” thereby increasing our sense of connection with and participation in the world. On the other hand, it has proved a veritable boon for the systematic spread of Dis- and Misinformation, Conspiracy Theories, and Boldface Lies, thereby fomenting distrust and disbelief in Democracy on scales

¹ Jamelle Bouie, “Facebook Is A Disaster For the World,” The New York Times, Monday, September 21, 2020, p. A25.

² See Ian I. Mitroff and Rune Storesund, Techlash: The Future of the Socially Responsible Tech Organization, Springer, New York, 2020.

previously thought unimaginable. Truth is not only under constant attack, but in abject danger of vanishing altogether. In too many cases, Social Media have shirked their fundamental Moral and Ethical responsibility by allowing outright lies to go unchecked for far too long and thereby to proliferate.

Gene-editing technologies promise the alleviation of countless childhood diseases. At the same time, it's given rise to the all-too-present fear that it can be used by rank amateurs to create veritable half-human monsters.³

AI can be used to help humans better navigate complex tasks and hopefully make more informed decisions. On the other hand, it can be used to create videos of prominent people saying and doing things that they never would but nevertheless fool experts as to their authenticity. Reality itself is in under constant attack. Who and what can one trust? To put it mildly, in the wrong hands, AI can lead to harmful decisions.

For another, AI fails seriously when it comes to incorporating diametrically opposed and conflicting patterns of thought. The plain fact is that there is not a single aspect of human existence that is not subject to widely different expert judgments and opinions. And yet, AI fails to incorporate this important facet of human experience. If anything, it embodies all of the biases and prejudices of its creators.⁴ We thereby question the "Intelligence" of AI.

We cannot continue on the same disastrous path of unleashing the most powerful technologies on the world and then later cleaning up their worst aftereffects, if we can indeed later. We have to get out in front by doing all that we can to anticipate the worst and then undertaking everything in our power to mitigate it, if not prevent it altogether. We have to plan for the fact that all technologies produce unintended side effects and negative consequences. Further, they can and will be systematically abused and misused by nefarious parties for ill ends.

As a result, let us outline and contrast two sharply opposing approaches to the Management of Technology. It's never been more important to compare and contrast these two. For want of better names, we call one the FDA Approach and the other Get-It-Out-the-Door ASAP.

The FDA Approach starts with the basic presumption that all Technologies are complex bundles of benign and potentially harmful and even dangerous properties. Furthermore, it's extremely difficult, if not virtually impossible, to ferret out and clearly distinguish between the two early on in the development and use of a Product/Technology. Intertwined with every set of benign, well-intended attributes and properties are Latent Defects and even Fatal Flaws. In addition, everything is capable of being abused and misused even by responsible users, let alone by disreputable parties who are deliberately out to cause as much harm and trouble as possible. Thus, even though it was not intended, and thus not planned for, Social Media has proved to be a perfect tool for Cyberbullying. It's also a perfect vehicle

³Jennifer A. Doudna and Samuel H. Sterberg, A Crack In Creation: Gene Editing And The Unthinkable Power To Control Creation, Mariner Books, New York, 2018.

⁴Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown, New York, 2016.

for the distribution of Conspiracy Theories and outright lies, not to mention direct interference in our elections.

Modeled after the strict, but not perfect, policies and regulations of the Food and Drug Administration, the FDA Approach mandates the scrupulous testing of a Product/Technology to expose as much as possible harmful effects and unintended ill consequences before it causes irreparable harm on an unsuspecting public. If a Product/Technology cannot be proven to be safe, then it is strictly prohibited from being released. Furthermore, testing is ongoing over its entire lifetime. It's never final or complete.

In sharp contrast, the Get-It-Out-the-Door ASAP Approach is exactly what its name implies. When it comes to potential problems, it's completely Reactive. Namely, since everything cannot be known beforehand, see what problems if any arise from the use of a Technology. In this way, one gets a hand up on the competition by releasing an innovation as quickly as possible. From the standpoint of Crisis Management (CM) whereas the FDA Approach is Proactive, the Get-It-Out ASAP is completely Reactive.

Of course, these two are archetypes since most organizations are a mixture of the two. Nonetheless, every organization leans more toward the one than the other.

Importantly, we know of two organizations which show unequivocally that it's possible to make thinking about the worst that can happen as a result of using their Products/Technology an integral part of their everyday operations. It allows them to pick up on major problems before they are too big to fix and thus turn into significant crises. In this way, instead of distracting from profits, it contributes substantially to them.

One uses In-House Internal Assassin Teams to attack and thereby find weaknesses in their products and manufacturing processes. The other uses a Chaos Team to do the same. In each case, they assume that they are in a perfect position to attack their products and processes because "they know more about them than anyone else." From their standpoint, they do indeed "know more than anyone else about their products and processes," but this does not mean that outsiders with completely different points of view should not be involved. Outsiders typically see things that insiders take for granted.

The point is that as much they are required, strict rules and tight regulations only work when we know or can anticipate the specific problems connected with Technology. In short, they need to be as detailed as possible. But when we lack such knowledge, we need other means—open-ended processes—such as Internal Assassin and Chaos Teams to help us be forever on the lookout for that which we cannot predict or know beforehand.

The point is that thinking about the worst cannot be left to chance or to the whims of a company if and when it feels like doing it. Similar to the FDA, it has to be enforced by a new Government Agency that will protect us from the worst abuses of Technology. Before any company is allowed to operate, it must show that it has planned for the worst and taken every step to prevent it. And, it must continue to do so over the entire course of its lifetime.

Ideally, planning for the worst is the cornerstone of The Socially Responsible Tech Company, indeed every company. However, given that Mitroff has a PhD in Engineering Science, he knows personally that such thinking is not uppermost in the minds of technologists. They are mesmerized by their wondrous creations, and thus primarily focused on them, not on their social consequences. Indeed, they overly hype the positive benefits and ignore and downplay the disbenefits.

We can no longer continue to reap the great rewards of Technology without planning and taking action against the worst. Doing it in a timely manner is in fact one of the predominant moral and ethical challenges of our times.

2.2 Proactive CM

Let us summarize the discussion thus far by emphasizing the key elements of Proactive CM.

Since with very few exceptions, all crises send out a repeated trail of Early Warning Signals announcing the highly probable occurrence of a particular set of crises, setting up mechanisms and procedures throughout an organization, institution, or society that will deliberately look for and record such signals is paramount. It's also necessary that such signals be transmitted to the right persons who have the authority to act on them in a timely and appropriate fashion. Above all, the messengers of bad news need to be rewarded, not "killed," as was unfortunately the case with the officials in Wuhan who first discovered the Coronavirus but were explicitly warned not to pass "bad news" onto their superiors in Beijing.

One of the best ways of ensuring the adoption of Proactive CM is to make it an integral part of a program that an organization already takes seriously. Thus, CM is a natural ally of Quality Control, not to mention Stress Testing, in order to surface, as best as one can, the underlying Latent Defects and Fatal Flaws in products and services. Quality Control and Stress Testing are also natural allies in surfacing the unintended consequences, and the abuses/misuses of a Technology, Product, or Service.

One of the most critical aspects of Proactive CM is uncovering harmful organizational Defense Mechanisms like Denial and fostering a corporate culture that works constantly to eliminate them as much as possible. To achieve this obviously requires Secure, Adult leaders. Lacking this, crises are virtually guaranteed to happen on a regular basis. For make no mistake about it, Denial will effectively kill any program in CM.

For example, early on Mark Zuckerberg was warned repeatedly by more than one subordinate that its enumerable crises—Cyberbullying, selling users' personal information, providing a primary means whereby foreign governments could interfere in our elections, etc.—were virtually guaranteed to happen. Not only did Zuckerberg suppress the warnings, but he actively discredited those who brought them. Worst of all, he labeled critics as "anti-Semitic."

For another, in the early days of the transition from President Obama to Trump, simulations showed in no uncertain terms that a major Pandemic was virtually guaranteed to happen. Unfortunately, President Trump did not take the warnings seriously. Indeed, he cut the budgets of major Public Health Agencies because they were a “waste of time and money.” After all, the worst didn’t happen. Denial big time!

And, while it’s finally come out that he privately acknowledged the seriousness of the Virus, he offered a flimsy excuse for downplaying it, namely, that “He didn’t want to panic the American people.” Given that he continually stirs up and stokes fears, it’s completely bogus.

Ferretting out potential crises is obviously important, but no less important are serious Mitigation Plans and Procedures.

For even with the best plans and procedures, crises still occur. Thus, Damage Control Mechanisms to limit their spread and resultant harm are essential. While each type of crisis naturally requires its own form (for instance, oil spills require physical barricades and cleanup dispersants to keep them from spreading), what’s absolutely crucial is that Damage Control Mechanisms cannot be invented in the heat of actual crises. The classic case is that of BP’s 2010 oil spill in the Gulf of Mexico. Millions of gallons were spilled from an errant well before it was capped. By then, incalculable damage was done to the environment.

Finally, every organization needs a fully functioning, full-time, and well-staffed Crisis Management Team or CMT. All of the senior officers of an organization need to be well-trained members of the CMT. In this way, all of the major corporate functions and specialties will be represented. Thus, since all crises invariably involve huge financial costs, the necessity of the Chief Financial Officer is obvious. But all crises involve serious legal issues, PR, etc. Furthermore, the CEO, or someone acting in his or her place, has to lead the team and give it the importance it deserves. Indeed, all of the members of the CMT need to be trained to step in and lead it.

The CMT needs to meet regularly to review both the status of potential crises and the adequacy of its programs in meeting the threats to the organization, its surrounding communities, the nation, and the world.

2.3 Concluding Remarks

The Coronavirus painfully shows how the world is susceptible to new crises all of the time. Unfortunately, Global Pandemics were not on the original list of crises. And, it painfully illustrates the Systemic nature of all crises, how something that originates in one country can quickly affect the entire world.

On February 24–25, 2020, the US stock market lost nearly 6% of its value, losing 2000 points on the Dow Jones. It was the biggest drop in 2 years. And, even though as of this writing in November 2020 the stock market has recovered, it only got worse in the days and weeks immediately following February. It still fluctuates

wildly as the Virus continues to wage. And while unemployment has also recovered, it's still dangerously low.

The world's economies and production facilities are inextricably linked. Thus, if China's manufacturing facilities are literally shut down, then it affects production worldwide. Further, if the Virus spreads to other countries such as Italy, then it damages the tourist industry.

It bears repeating: Each and every type of crisis is linked to every other one in predictable and unpredictable ways. Thinking the Unthinkable via Worst-Case Scenarios has never been more critical.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.