The Socially Responsible Tech Company

6

[The global information war] is a war without limits and boundaries, and one that we still don't know how to fight. Governments, nonstate actors and terrorists are creating their own narratives that have nothing to do with reality. These false narratives undermine our democracy and the ability of free people to make intelligent choices. The disinformationists [sic] are aided by the big platform companies who benefit as much from the sharing of the false as from the true....Autocrats have learned the same tools once seen as spreading democracy can also undermine it...

Stengel [1]

Proactive Crisis Management (CM) is the backbone of the Socially Responsible Tech Company, SRTC. From its very inception and across its entire lifespan, Proactive CM needs to guide its every action, indeed it's its *Raison d'Etre*. A SRTC would therefore be constantly on the lookout for the unintended consequences of its technologies, how they can be abused and misused, and how they can be minimized if not prevented altogether. The primary emphasis is on constantly monitoring for harmful effects and ill consequences.

For this reason alone, we review the essential elements of Proactive CM.

Types

The first element of Proactive CM is not only planning, but being prepared for a broad range of different types of crises. Previous research has shown that there are distinct families or types of crises.¹ Thus, there are informational crises as when

¹Mitroff [1].

unauthorized parties hack into supposedly secure systems and steal highly personal information such as social security, credit, and health data. There are financial crises as in the case where the finances of an institution are mismanaged or subject to criminal malfeasance. There are Public Relations, PR, or reputational crises. For example, Volkswagen caused a huge PR crisis for itself when its concerted efforts to deceive the public with regard to the true values of the pollutants emitted by its cars came to light. Needless to say, Volkswagen's reputation took a severe hit. There are ethical crises as in the case of the Catholic Church where those who are guilty of serious sexual crimes against minors are not brought to the immediate attention of the proper legal authorities. Human Resource or HR crises include deliberate acts of Employee Sabotage. The intentional abuses and misuses of products are contemporary instances of Product Tampering. Natural Disasters are another major category. So are Fires and Explosions. And in today's world, International and Domestic Terrorism are always worrisome possibilities.

These do not by any means exhaust the full range of the possible types of crises for the world is unfortunately continually inventing new ones. Nevertheless, they are sufficient to give a good feel for the different types and the wide range of crises.

Most important of all, while the different types are distinct in that they can be clearly identified and labeled as such, they are not independent. Time and again, it's been shown that *no crisis is ever a single crisis*. Every crisis is potentially both the cause and the effect of every other. A crisis may start in one category or type, but it quickly spreads to all of the others. If one is not prepared, it sets off an uncontrolled chain reaction. Thus, to reiterate, Volkswagen's emission crisis was a HR crisis in that it involved groups of employees up and down the corporate hierarchy. It quickly became a major PR and a financial crisis for the company as whole. In short, all of the various "types" are elements of a Mess!

The key point is that preparing for a limited number of crises is not only inadequate, but actually increases the crisis potential of an individual, organization, society, and in today's world, the entire planet. In brief, it is counterproductive. In fact, it leads to feelings of false security. For this reason, Proactive CM is fundamentally systemic.

All of the aforementioned types apply equally to tech companies. However, in addition, the various types of the Unthinkable are applicable as well. Indeed, they are intertwined. Thus, knowingly and unknowingly, the assumptions that are made about unanticipated stakeholders come back more often than not to haunt one in the form of major crises. Nonetheless, by far, the most dangerous have to do not just with Product Tampering, but with product defects such as latent defects and fatal flaws.

Recognizing and preparing for a broad range of crises ideally leads to setting up specific mechanisms and procedures for the detection of the Early Warning Signals that not only accompany, but precede all crises. Since different types of crises send out different kinds of signals, each crisis calls for its own distinct form of devices and procedures for Signal Detection.

To make CM truly effective, it needs to be an integral part of a company's everyday operations. One of the best ways of doing this is to make it a key part of an already existing program that the organization currently takes seriously such as Quality Control. In fact, Quality Control is a natural home and ally of CM.

Damage Containment and Mitigation

One of the most critical parts of Proactive CM is Damage Containment. And, different types of crises involve different types of Damage Containment Mechanisms and Procedures. What is appropriate for one doesn't necessarily work for others. Thus, a protective barrier designed to keep a fire or oil spill from spreading will not keep a financial crisis from eventually engulfing and destroying an organization. Financial crises necessitate among other things safeguards such as independent auditors and whistleblowers.

One of the most important things about Damage Containment Mechanisms and Procedures is that they cannot be invented in the heat of an actual crisis. BP's 2010 oil spill in the Gulf of Mexico is dramatic testimony to this unfortunate fact of life. Millions of gallons of oil were spilled leading to untold environmental damage and destruction before the errant well was finally capped. Again, the operative words are systemic and proactive.

Ideally, both Signal Detection and Damage Containment direct one to focus on Mitigation. It raises the question as to what one can do to design and redesign one's products and manufacturing processes so that the possibilities of major crises are greatly reduced, if not prevented altogether, and further, that the ultimate goal of ensuring the safety of those who can be potentially harmed is a major priority.

Defense Mechanisms

One of the most critical but unfortunately least discussed factors in the typical accounts of CM are Defense Mechanisms. If Sigmund Freud had done nothing more than discover the existence and functioning of Defense Mechanisms, it would have been more than enough to ensure his lasting fame.

Defense Mechanisms basically exist to protect the minds of individuals from painful events and harmful memories that are too difficult to acknowledge consciously. Thus, if one has been in a war and witnessed the death of a fellow soldier or companion, then one can attempt to shut the entire event out from consciousness through Denial, i.e., by denying that the entire event ever occurred in the first place. The same applies if one has been the subject of a violent attack or incident. Unfortunately, since Denial is never perfect, the repressed event often comes back in the form of nightmares from which the combatants in war typically suffer. Unfortunately, fire and police personnel typically experience this as well.

Early on as one of the key founders of the modern field of CM, Mitroff and his colleagues discovered that there were direct organizational counterparts for every one of the Defense Mechanisms that were originally discovered and which pertained solely to individuals. Thus, in organizations, Denial often takes the form, “We don’t have any major problems.” With regard to technology, “Our technology will work as intended with no major problems or issues.” For another, “Nefarious, malicious actors are not a problem about which we need to worry.” “It’s a total waste of time and money to Think about the Unthinkable, let alone plan for it.” Or, “Despite all the fears and protests, people have always adapted before to new technologies so that there are no serious reasons to believe that we won’t do it again. In other words, present concerns are largely overblown.”

Disavowal takes the form, “Yes, there are problems, but they are minor. They are not important enough to warrant major attention.” Disavowal thereby reduces the complexity, magnitude, and scope of problems and issues to where they can supposedly be downplayed and thereby ignored. Once again, “Fears about technology are greatly overblown.”

Projection takes the form, “Someone else is to blame for our problems, not us.” In other words, “We’re not responsible for problems in any way.” In the case of technology, “We’re not to blame for those who abuse and misuse our technologies.”

Intellectualization is the attitude that “Our technology is perfect.” Or, “We can catch all problems before they are too big to handle.” For another, “We’ve thought of everything that could possibly go wrong and planned for it so there’s nothing to worry about.” As such, it’s obviously intertwined with Denial, as are all of the various Defense Mechanisms.

Compartmentalization is the attitude that “A crisis may affect parts of an organization or a technology but not the whole of it.” Compartmentalization thus avoids thinking and acting systemically. Crises can thereby be confined as a result.

Grandiosity takes the form, “We are smart, powerful, and competent enough to handle anything!” Again, “We’ve thought of everything.”

Finally, Idealization is the attitude that “Everything will work as planned.”

It’s been found that the more that an individual or organization subscribes to the Defense Mechanisms outlined above, the more crises they experience. Thus, instead of protecting one, Defense Mechanisms do the exact opposite. Once again, a key element of Thinking the Unthinkable is seriously contemplating how all of one’s idealized assumptions can lead to their direct opposite.

Ultra-proactive

If the idea of a Tech Court is a prime example of an *external* mechanism for helping to ensure that technology will serve us well by causing no harm, then the following is a prime example of a company that did everything that it could *internally* to help ensure the safety and well-being of its consumers.

Not long after the 1982 Tylenol poisonings, which was the impetus for among other things for the creation of the modern field of CM, Mitroff established The USC Center for Crisis Management, the first academic institution of its kind to study crises of all kinds. The basic purpose of the Center was to do research so that hopefully future crises could be handled better, if not prevented altogether. To further knowledge about CM, the Center had corporate sponsors who not only provided funds for its work, but just as important, gave unfettered access to their organizations so that Mitroff and his colleagues could study how they both prepared for and responded to various types of crises.

In the hopes of learning more about Product Tampering, one of the most important types of crises that apply to all organizations no matter what their business, Mitroff visited a major pharmaceutical company (It's important to stress that with regard to tech, Product Tampering takes the form of the systematic abuse and misuse of technologies.). Mitroff asked the person who agreed to talk with him what his company was doing to combat the ever-present threat of Product Tampering, a major cloud that perpetually hung over the entire Pharma industry. Without losing a beat, he said, "We formed a number of Internal Assassin Teams." To which Mitroff blurted out, "You did what?!"

Yeah, early on we realized that we knew more about our products than anyone else. So one day we held up a bottle of one of our major pain killers and we looked at it as if the cap were the front door and the sides were the walls of a house. We then asked ourselves, 'How could a burglar get in, remain undetected for as long as possible, and thereby do the most damage?'

We quickly learned that there was no way to keep a determined burglar out so that the notion of tamper proof seals was not even a remote possibility. The best we could do was tamper evident seals so that if one of our bottles was breached a consumer would be alerted not to use it.

In the years since, Mitroff has taken a few companies—sadly, all too few—through the exercise of an Internal Assassin Team as it applied to their organization. It allowed them to imagine and thus confront the all-too-real possibility of the worse, the Unthinkable, happening to them and their company. The point is that one needs explicit permission to imagine the worse and then to do everything possible to prevent it. Thinking the Unthinkable does not happen naturally on its own.

Risk Management RM

If only for the reason that RM is often confused with CM, it's imperative that we say a few words about it. The two are definitively not the same.

RM is based on the concept of Expected Value or EV, which derives from the theory of Probability. To take an overly simple example, if we have an unbiased coin, one for which the probability of getting a heads is $\frac{1}{2}$ and is the same for a tails, then if we throw a coin 100 times, we would expect to get 50 heads and 50 tails. Suppose every time we get a heads we win \$1 and every time we get a tails we lose

\$2. Then, we would expect on average to get $50 \times \$1 - 50 \times \2 or to lose \$50 in 100 tosses. The formula is $EV = \text{The Probability of Event One} \times \text{The Payoff or Loss of Event One} + \text{The Probability of Event Two} \times \text{The Payoff or Loss of Event Two}$, where there can of course be more than just two events and outcomes.

There are at least four possibilities with this supposedly simple procedure:

1. We know both the exact probabilities and outcomes or consequences of an event;
2. We know the probabilities but not the consequences;
3. We don't know the probabilities but we know the consequences.
4. We know neither the probabilities nor the consequences.

Case 1 is the prototype of an exercise where everything is supposedly known or given. As we've indicated, this is rarely the case. Indeed, it really happens only in textbooks.

Case 2 is best exemplified by wildfires. While the probabilities are not known exactly, wildfires are nearly certain to occur in every fire season in the Western States. It would be the extremely rare season in which there was not at least one major fire. And, while the consequences from previous years are known, they vary dramatically from year to year.

Case 3 typifies earthquakes where the consequences are known to be high, but when and where a major earthquake will occur is "problematic."

Case 4 is that of Wicked Messes. It also typifies "Unknown Unknowns." That is, where in cases 2 and 3, We Know What Don't Know, in case 4, We Don't Know What We Don't Know.

Unfortunately, RM contains even greater defects. First of all, it's rarely systemic in that typically one doesn't consider how one risk can set off a chain reaction of others as is the case with CM. Second, it does not take into account Defense Mechanisms, which prevent far too many organizations from engaging in RM and CM in the first place.

Also, RM does not take into account that we don't experience the Expected Value of an event but the actual costs. Thus, while the probability of a \$1,000,000 house burning down in a particular area may be low, say 1 in a 1000, the replacement cost is not 0.001 times \$1,000,000 or \$1000 but more likely \$1,200,000 and up.

For these and other reasons, we are not champions of RM. If RM is done at all, we insist that it be part of a broader, concerted effort in CM.

One of the saddest aspects of the whole issue of Crisis Preparedness is the fact that at best only 10–15% of companies have anything approaching a viable, let alone ideal, program in CM. This is in spite of the fact that those companies that are Crisis Prepared not only experience substantially fewer crises, but are significantly more profitable. If ever there was testimony to the power of Defense Mechanisms, namely "We don't have any problems for which we need to prepare," etc., this is it!

The Need for Systemic Thinking

Finally, we want to conclude this chapter by emphasizing once again the systemic nature of CM. The best way to do this is by understanding the kind of Inquiry System (IS) that is the foundation of Proactive CM.

The History of Philosophy recognizes at least five different and distinct methods of Inquiry (Inquiry Systems or IS's) for gaining knowledge if not the Truth²:

1. Expert Consensus or Empiricism;
2. Analytic Modeling or Rationalism;
3. Multiple Perspectives;
4. Conflictual Modeling of Dialectics; and
5. Pragmatist or Systems Thinking.

The first model or IS is predicated on the agreement between different experts. That is, the tighter the agreement between the assessments of set of independent, recognized experts with regard to the “Facts” of a situation, the more that the “Facts” are the Truth. The latest incarnation of this IS is “Big Data” which forms the basis of algorithms which are in turn the basis of AI programs.

The second IS asserts the primacy—indeed, superiority—of Single Analytic Models over data no matter how big the datasets are. In this way, the first two IS's are best suited to exercises where problems and issues are well-defined.

The third IS is based on the strong presumption that no single group of experts or model is ever sufficient to capture a situation fully. The more complex and critical the situation, the more we need to see how it appears to different stakeholders—indeed how they “represent it.” At the least, we need to negotiate the different perspectives of different experts. Thus, to take an important case, we wouldn't expect a social worker, a psychologist, a medical doctor, parent, etc. to have the same view of drug addiction, let alone how to treat it successfully. It's not that one perspective or viewpoint is right and the others are wrong, but that all of them are merely picking up “One Aspect Of A Complex Truth.”

The fourth IS says that we need to have the strongest debate we can muster before we decide a critical situation, as in the case of the Airman in Alaska who had a debate with himself as to whether the “large object coming over the horizon” was actually a swarm of enemy missiles or not.

As we have stressed repeatedly, all of the issues connected with tech deserve the strongest debate to which we can subject them. To take a single case, with regard to the Claim that Social Media can and should speed up conversations—more importantly, decision-making—the counterargument is that to further deliberation and reflection, Social Media should be slowed down. If not, it does not necessarily lead to positive outcomes.

²See Mitroff and Linstone [2].

Finally, the last IS is the foundation for Systems Thinking. It insists that all problems of any importance are parts of Wicked Messes and must be understood as such. Accordingly, it's the foundation of the thinking and behavior of the Socially Responsible Tech Company.

References

1. Mitroff II (2005) Why some companies emerge stronger and Bteer from a crisis: 7 essential lessons for surviving disaster. Amacom, New York
2. Mitroff II, Linstone HA (1993) The unbounded mind, breaking the chains of traditional business thinking. Oxford University Press, New York

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.