genium&co

Inspiring Excellence

Genium & Co is honoured to have Mr. Eric McNulty, Associate Director and Program Faculty at the National Preparedness Leadership Initiative (NPLI), local experts and experienced practitioners share their insights on crisis leadership at the Genium Leadership Symposium 2019.

Specially written for the Genium Leadership Symposium 2019, this white paper covers the concepts of Meta Leadership, Swarm Intelligence, Psychological Safety, Crisis Communications, POP-DOC loop to better prepare leaders to lead effectively and uphold the organization's reputation during crisis.

You’re It: Meta-leading through Crisis

By
Eric J. McNulty, M.A.
Associate Director
National Preparedness Leadership Initiative

Co-author, *You’re It: Crisis, Change, and How to Lead When it Matters Most*

July 2019

National Preparedness Leadership Initiative

A Joint Program of the Division of Policy Translation and Leadership Development, Harvard TH Chan School of Public Health and the Center of Public Leadership at the Harvard Kennedy School of Government

INTRODUCTION

We live in turbulent times. From product failures to terror attacks to natural disasters to cyber-crime, organizations and their executives face a diverse array of risks and threats. Some are well-known. Others are emergent, presenting novel challenges. The job of leaders is to keep themselves and their teams grounded, productive, and adaptive as they navigate across a treacherous landscape.

Effective preparedness for and response to many of these challenges goes beyond technical processes and protocols. Leading is rooted in human factors: motivating, guidance, achieving cognitive clarity, and modeling emotional intelligence. Lack of a coherent crisis strategy and vision, fights over budgets, disagreements about accountability, government agency rivalries, competitive concerns among businesses, and of course, egos and institutional pride all contribute to the problem. Media attention also amplifies the pressure for executives to move quickly. Understanding how to lead in such a high-stakes, high pressure environment as a response is a required core competency for all executives and those who support them.

When a company has an emergency manager or security chief, he or she will need support to handle the many technical aspects of the response. Where there is no executive, which is the case in many companies, someone without specialized training or knowledge may have to step up. In any event, other executives will need to lead other aspects of the response that affect customers and employees.

The enduring challenge is that many executives have not yet fully grasped the complexities of what they will face. When you don't fully grasp the threat, it becomes harder to have confidence in your response. This can result in hesitancy, bickering, second-guessing, and other negative behaviors that can degrade performance. Conversely, when managers are trained and have exercised sufficiently, they will move surely through even the most difficult of challenges. We offer the meta-leadership framework and practice method, developed over more than 15 years of crisis leadership research, to help leaders achieve the best possible outcome in trying conditions.

ANY CRISIS TESTS EXECUTIVES

Crises put managers to the ultimate test: “Facts” on the ground change quickly. Senior executives, board members, investors, and the media demand instant answers… and can begin pushing ill-advised solutions if they are not satisfied. Suddenly, everyone is an expert. Plans, no matter how carefully crafted, invariably fail to anticipate every contingency. Organizational structures often must shift into crisis mode to get the right people in the right places. External advisors may join the team. This may require relationship building on the fly as people who don't ordinarily work together are thrust side-by-side. The adaptive capacity of the organization and its executives is challenged as they work to determine what exactly has happened and how best to respond. Effective leaders are essential to create unity of effort, nimble decision making, and highly coordinated cross-functional activity.

Leading in a crisis requires enough understanding enough about the technical issues to work with the relevant internal and external subject matter experts. Just as important, leaders must understand the human dynamics necessary for high performance of the many individuals and teams who will be deployed to handle the varied facets of a response. In short, leading is much more about behaviors than title. My colleagues at the National Preparedness Leadership Initiative (NPLI) and I developed the meta-leadership[1] framework and practice method to consolidate these insights and best practices.

We've seen these challenges firsthand, studying leaders in extreme consequence situations from the H1N1 pandemic to the Deepwater Horizon oil spill to the Boston Marathon bombings, as well as helping teach civilian and military executives around the world. This report outlines central concepts and practical tools for understanding brain function, human behavior, and other facets of crisis leadership derived from more than 15 years of research and practical application of the findings in a wide range of crisis settings.

Meta-leaders take a broad, holistic view of an incident. The think and act across three dimensions: The Person, incorporating self-knowledge and self-awareness including their strengths and limitations; The Situation, discerning a nuanced understanding of what is happening and, therefore, what to do about it; and Connectivity, building robust relationships within and across organizational boundaries that link and leverage people, expertise, and physical resources to increase the potential of the best-possible outcome. That connectivity is built by leading “down” to one’s team; “up” to one’s boss; “across” organizational boundaries; and “beyond” to entities beyond one’s own.

[1] Marcus, L., Dorn, B., Henderson, J., and McNulty, E. (2015). Meta-leadership: A Framework for Building Leadership Effectiveness. Retrieved on June 19, 2017 from https://npli.sph.harvard.edu/resources/

GREAT FOLLOWERS ARE ESSENTIAL TO GREAT LEADERSHIP

While many stories about crises handled well focus on a principal protagonist, the “leader,” few such outcomes are the result of the actions of a single individual. Generals do not win battles by themselves and neither do CEOs. The person at the top has a critical role to play in establishing focus, setting the tone, and making high-consequence decisions, he or she is dependent upon many other people to deliver accurate, timely information, proactively solve problems at every level of the enterprise, and offer alterative perspectives on what is unfolding as well as innovative ideas on what to do. We have found that the best crisis leaders are both confident and humble. They believe in themselves and their teams yet never so much as to think that they have all of the answers or that they fully grasp the perspective of every stakeholder. Cultivating great followers is a primary endeavor of effective leaders.

My colleagues and I saw this in the response to the Boston Marathon bombings in 2013. The senior-most executives from the various agencies were almost all away from the scene at the time of the bombings. They consistently reported calling their second-in-command and, as soon as they established that this person was on scene and that operations were functioning, they could pull back to look at the bigger picture and its implications. They could concentrate on connecting with their peers to ensure a coordinated response. This, in part, is why that operation was so effective.

One of the key “leading up” challenges for followers is keeping senior executives out of the weeds regarding the incident. When the boss is confident that the details are being attended to, he or she can more easily pull back to see the big picture. The c-suite and the board will need periodic updates. They need to know what's going well and where roadblocks have been encountered in order to keep their key stakeholders well-informed—an essential part of creating the space for operating teams to do their work. However, if the c-level executives start micro-managing the work of vice presidents and others in the response effort, overall team function is certain to decline as decisions will hit bottlenecks, subordinates will pull back from offering new ideas, and corrosive second-guessing will consume valuable time and energy. Followers who are credible and reliable will have the trust of the senior team.

It’s more than managing your boss, you need to lead him or her so that they can best prioritize decisions, allocate resources, manage peer relationships, and, perhaps most important, lead their boss in turn. A great follower helps do this by anticipating what the boss will need next. It is how you want your team to lead up to you. One Chief Information Security Officer (CISO) interviewed for this paper shared a “battle-tested” briefing framework that he has used to lead up successfully for years:

- An incident overview (because new people are often added to the distribution list over time)
- Incident response goals (make sure the objective is clear to prevent working at cross-purposes)
- Facts/Finding (distinguish between what you *know* and what you *think*)
- Analysis and Opinions (help people understand what the data means)
- Recommendations (include “why,” not just “what”)
- Actions Taken (give credit widely)
- Actions Pending (along with who owns them)
- Resourcing (personnel, equipment, finance)

A suggested addition to this is “help needed/requested” so that those beyond the technical response team know how they can most productively assist. Such a briefing will help “feed the beast” of executive inquiry. One company with which we’ve worked stanches the flood of update request by scheduling morning and evening briefings with the promise of an immediate interim brief should something of significance transpire. It may be useful to assign people from the employee communications team to compile such a report in order to take some burden off those who in the throes of the actual response. This person or team could also add a brief summary feedback received from internal and external stakeholders. The goal is to facilitate the flow of information that will foster decision making and action taking across the enterprise.

A great boss, in turn, will share the questions and concerns they are hearing from their peers, the status of engagement with outside resources from law enforcement to crisis communications, legal, digital forensics, and other external resources. Each of these parties brings resources, expertise—and often their own ideas on how to run the response. The best way to preserve your sanity and the cohesiveness of the team is to understand the psychological and behavioral mechanisms at play.

To foster the conditions for high performance in a crisis, focus on these six basics:

- Understand how the brain works under stress
- Foster an environment of psychological safety
- Establish positive behavioral norms
- Develop a multi-dimensional situation map
- Focus on communication
- Cultivate a proactive system

Understand How the Brain Works Under Stress

All humans have an automatic threat response—freeze, flight, fight—that dates back to our days avoiding saber-toothed tigers and other pre-historic threats. It is known as the “amygdala hijack”[2] or “going to the emotional basement.”[3] This is a place of panic, rash action, and emotional outbursts. This reaction is triggered when someone cuts you off on the highway, when you hear an analyst downgrade your stock, or when the telephone rings in the middle of the night. In the face of any perceived threat, the brain is hard-wired to go into survival mode. Upon hearing of the loss of substantial customer data, threatening legal action, or other incidents, most executives will descend rapidly to the emotional basement.

To climb out, your first job is to recognize this basement state and take steps to counteract this in yourself, your boss, the team, and the rest of the organization. This is accomplished by undertaking a task at which you can demonstrate self-competence: Take three deep breaths, count to 10, or activate a practiced protocol. Once the brain senses ordered, controlled activity, it resets—almost like rebooting a computer—and productive thinking can return.[4] Once calmed yourself, you can assign tasks to the team and others to get them out of the basement. It matters less if it is precisely the right activity than that it is one that people can execute using a deep-seated learned behavior. The team has likely drilled protocols for undertaking anticipated risks. Set them to it. Even asking someone to make coffee can serve the purpose. Only by going through this calming reset process will people be able to rise up to the creative thinking and complex problem solving needed to move forward. If you have new team members, reminding them that you’ve “been there, done that” can be calming as can expressing your confidence that the team will succeed.

Perhaps the hardest people to whom to assign tasks are the boss and members of the senior executive team. Still, it is essential that they get out of “the basement” lest they hinder the response. Involving executives in preparedness drills will help the response leader better understand the questions they will ask, the information they will want to receive, and the decisions they anticipate they will have to make. In an actual response, involve them in setting and prioritizing the goals for these efforts. One senior security

[2] Goleman D. *Emotional Intelligence: Why it can matter more than IQ.* 10th anniversary hardcover ed. New York, NY: Bantam Dell; 2006.

[3] Ashkenazi I. Psychology and actions of the crisis leader. Harvard University, Cambridge, MA: Presentation at the National Preparedness Leadership Initiative; 2007, March 9.

[4] McNulty, E. & Grimes, J. (2016). “Rise to Better Leadership: Using the ASCEND Model to Improve Crisis Response,” National Healthcare Coalition Preparedness Conference, Washington, DC, December 12-14, 2016.

executive shared with me that this gets executives to “start thinking critically and like leaders again.” With this knowledge, it is possible to keep everyone focused and productive.

Foster an Environment of Psychological Safety

The complexities, uncertainty, and ambiguity in the immediate aftermath of an incident can unsettle even the steeliest of executives. The human brain prizes coherence even in the absence of evidence[5] which can lead to hasty decisions and blame throwing in the quest for certainty. Research by Rock[6] has shown that the brain processes social pain in much the same way that it handles physical pain so blustery finger-pointing can have the same effect as a slap to the head. That is sure to degrade team performance exactly when you need your people to be at their best.

Instead, articulate your confidence in people to get the job done. Simply saying, “We can do it,” can help restore the necessary confidence to meet the challenges at hand. This is good policy in preparedness as well. Research by Edmondson[7] demonstrated that in environments where mistakes can be admitted and discussed openly, fewer mistakes get made and people are more willing to offer new ideas. If you want people to take chances, you have expect them to fall short from time to time. Use a failure, particularly a non-catastrophic failure, as a chance to learn and improve.[8]

It is useful to take a page from the patient safety movement in health care[9] where a core principle is first to look at the overall system in the event of an adverse outcome. Effective system design, training, and resourcing are the responsibility of the organization: Do people know what to do? Do they have the time and tools to do it right? Are they encouraged to point out vulnerabilities without fear of ridicule? Are they empowered to be a voice for the standards of the system regardless of their rank or role? Only after determining that the system itself was not the source of failure do investigators look at the roles of the individuals involved. This mitigates blaming and instead focuses on solving problems. This system-based

[5] Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus, Giroux.

[6] Rock, D. (2009). Managing with the Brain in Mind. *Strategy + business*, 56, 1-11.

[7] Edmondson A. Psychological safety and learning behavior in work teams. *Administrative Science Quarterly.* 1999;44(2):350-383.

[8] Danner, J. & Coopersmith, M. (2015). The Other “F” Word: How Smart Leaders, Teams, and Entrepreneurs Put Failure to Work: Wiley: Hobobken, NJ.

[9] Emmanuel, L.., Berwick, D., Conway, J., Combes, M., Leape, L., Reason, J., Schyve, P., Vincent, C., Phil, M., & Walton, M. (n.d.). “What exactly is patient safety?” Agency for Healthcare Research and Quality. Retrieved on March 1, 2017 from https://www.ahrq.gov/downloads/pub/advances2/vol1/Advances-Emanuel-Berwick_110.pdf

mindset and approach has greatly reduced avoidable errors in health care and there is no reason that it cannot do the same in IT security.

Together, these steps should help reduce vulnerabilities as well as foster rapid, coordinated action in the event of an incident. Rather than running for cover, people will jump into the fray.

Establish Positive Behavioral Norms

My colleagues and I saw unprecedented intra- and inter-organizational coordination and collaboration in the aftermath of the Boston Marathon bombings in 2013. As we interviewed many of the individuals involved and studied their decisions and actions, we saw five consistent behavioral norms emerge:

1) Unity of mission

2) Generosity of spirit and action

3) Staying in one's lane

4) No ego, no blame

5) A foundation of trust-based relationships

We call this "swarm leadership"[10] with reference to the swarm intelligence[11] of species such as bees and ants. It isn't as crazy as it sounds—these five behaviors help optimize performance within existing protocols and procedures while facilitating adaptation to unforeseen and changing circumstances.

Unity of mission is alluded to in the incident brief recommended above. Part of a leader's job is to get people on the same page. While that may seem easy, in the aftermath of a cyber security incident, some will be thinking about getting the bad guys, others worry about reputation or financial damage, and yet others fortify themselves for potential litigation. Some people will worry about their careers. People get

[10] Marcus, L., Dorn, B., McNulty, E., and Goralnick, E. (2014). Crisis Meta-Leadership Lessons from the Boston Marathon Bombings Response: The Ingenuity of Swarm Intelligence. Retrieved on June 19, 2017 from https://npli.sph.harvard.edu/resources/

[11] Miller, P. (2007, July). "Swarm Theory: The Genius of Swarms," *National Geographic*. Retrieved on June 19, 2017 from http://ngm.nationalgeographic.com/2007/07/swarms/miller-text

pulled in many directions. Your leadership challenge is to articulate a compelling mission that will bring focus to the situation. For example, “minimize negative consequences for our customers” will help different functions set priorities and begin to move forward.

Generosity of spirit and action means helping each other out. That may mean putting aside departmental rivalries to leverage each other’s resources. It may mean offering people to cover business-as-usual tasks to free up resources for the response. Even making a coffee run for those in the emergency response team can help.. It may even extend to offering to feed the cats and walk the dogs of the crew working around the clock on the incident.

There can be tendency for everyone to cluster around the technical issues as they want to be in on “the action.” It can be like a grade school soccer game where all of the players chase the ball rather than playing their positions. It is important for people and departments to attend to their principal function—stay in their lane—in order to ensure all of the essential work of the organization continues while the information security team has the time and space to do their jobs.

No ego and no blame may be the toughest of the five behaviors to maintain over time. There is a natural inclination to want to determine what went wrong and point an accusatory finger at those who may be at fault. Similarly, alpha personalities want to assert themselves—“I’m in charge!” None of that is useful. As a leader, you want as many people productively engaged in the response as possible. There will be time for accountability in the after action review. In the heat of the response, give credit widely, praise collaboration, and provide sufficient top cover to allow those working for you to focus on the task at hand. You likely won’t be the one to solve the problem but you can be the one who creates the conditions under which the team rises to the challenge.

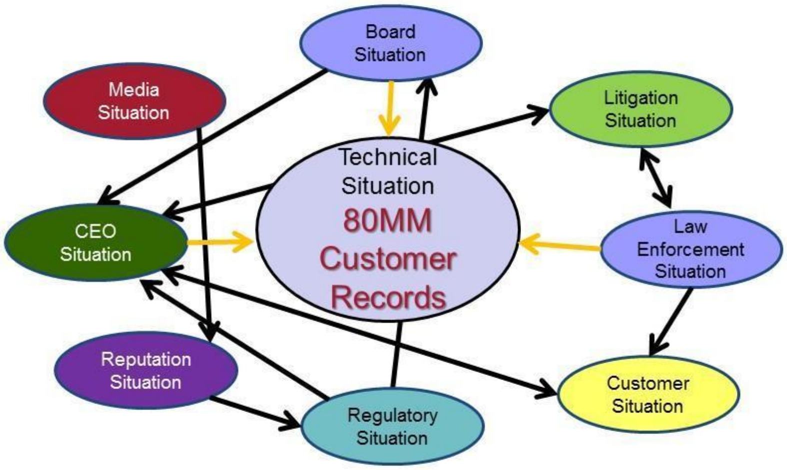
Perhaps most important is a foundation of trust-based relationships. These cannot be forged in the moment but rather must be built over time. Managers must fight the tendency to hunker down in the “bunker,” interacting only with their functional colleagues. Exercise your leadership to connect with your peers across the organization and encourage those who work with you to do the same. The relationships in Boston were fostered over more than a decade of cross-sector, multi-organizational exercises and drills. One of the major advocates for private sector participation in crisis preparedness in Boston hosts an annual exercise to which local, state, and local representatives of federal agencies are all invited. In a few hours’ time and for the cost of coffee and bagels, bonds are formed and best practices shared. This should not be as unusual as it is.

As a leader, you can model these behaviors. You can recognize and reward them in the people who work for you. You can encourage them in your peers and colleagues. As swarming occurs in nature, it can be intentionally encouraged to emerge in your organization.

Develop a Multi-Dimensional Situation Map

The situation map (see Figure 1) is built starting with the technical situation and asking two questions: What does it influence? What influences it? The answers to these questions will reveal the various component situations as well as the relationships between them.

The Situation Map: HealthCo



There are *Multiple Situations* in Which You Must Lead

No one executive or manager will be responsible for each of these but every leader involved needs to know what is in play, who is attending to it, and what impact those dynamics might have on the aspects of the response in which they are involved. For example, an incident that receives media attention will have different time pressures than one that goes unmentioned in the news. In the Deepwater Horizon oil spill response, the battle over “optics” between local and federal officials played out in dueling appearances on live television and drove some operational decisions that were later criticized.[12] The involvement of state or state-sponsored actors, as was seen in the Sony incident, can create distracting political dynamics that will reverberate with senior executives and investors.

For each of these situations, those responsible should articulate to stakeholders, their likely orientation (for you, against you, or neutral), and their level of influence. Plans can then be made to leverage allies and mitigate detractors. Such an exercise makes for an excellent non-technical drill or exercise that will ensure that financial, legal, marketing, investor relations, human resources, and other colleagues know what is expected of them—and what they will expect of others. Set a scenario and assume that your technical protocols are unfolding as planned. Concentrate on the impact on everyone else. In an actual incident response, building a situation map can serve as the brain reset task to get you or someone else out of the emotional basement.

It is never easy to get the attention of these busy executives. Rather than pepper them with your latest defensive brainstorm, initiate a conversation with questions, perhaps spurred by the latest incident highlighted in the media, about what they anticipate their concerns and questions will be at zero hour and then plus three, six, 12, 24, 48, and 72 hours. What are the most critical situations? Who are likely to be the most important stakeholders and what will be their concerns? Having some understanding of these priorities and dynamics in advance will help everyone retain focus in the midst of a true incident.

Provide lunch if that’s what it takes. This a way to gather valuable information about the business issues and elevate your stature as a leader with insights about customers and the business, not simply safety and security issues.

Communicate, Communicate, and Communicate Some More

Effective communication is the lifeblood of a productive crisis response. Leaders at all levels should think broadly about the emerging narrative. The situation map provides guidance regarding constituencies and their concerns.

[12] National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2011). *Deep water: The Gulf oil disaster and the future of offshore drilling*. Retrieved from http://www.gpo.gov/fdsys/pkg/GPO-OILCOMMISSION/pdf/GPO-OILCOMMISSION.pdf

With internal constituencies, those from specialized functions must be careful to "code shift" when communicating with those from other silos who may find their jargon and acronyms completely foreign. In the pressure-filled environment of a response, clear communication is critical to success—even if that means slowing down a bit to ensure that you are not just heard, but understood.

Though the leader may be relying on internal or external communications professionals, and should generally heed their advice, it helps to know some “Crisis Comms 101” in advance:

- **Tell executives what you know (and can legally disclose).** Tell them what you don’t know. Tell them what you are doing find out what you don't know. Where possible, tell them what they can do. This simple framework is a reliable guide for a variety of incidents. It focuses the organization on proactive, iterative communication and demonstrates both concern and a bias for action. The final step helps keep affected parties out of the basement.

- **Encourage the communications group to develop a general holding statement well in advance and have it cleared by the legal and other relevant departments.** A first statement to the press will be fairly short and generic because there likely will not be many confirmed details available. Something along these lines is generally sufficient for an initial statement:

  > “Acme Corporation has become aware of a potential breach of its information systems. We have expert internal and external resources and are working with law enforcement and other relevant officials to determine the extent of this incident. The protection of customer and employee data is a priority for Acme Corp and we will take the appropriate actions that our customers and our investors should expect. We will provide addition information as we know more.”

  Follow the guidance of communications professionals on if and when to engage the media.

- **It is easier walk back a number than to dial it up.** Recall the mine disaster in Chile in 2010. Thirty-three miners were trapped underground in early August. As rescuers settled in for a long recovery effort, the President of Chile said that he hoped that the trapped miners would be out by Christmas. When they were rescued in October, the President and the rescuers were heroes in part because they beat their self-imposed deadline. When you set expectations about amount or type of data, number of parties affected, etc., do it so that you have room to over-deliver in your response. Such an approach helps protect your reputation for competence and may lessen pressure from the media or board for an immediate fix.

This is also true of the numbers of affected parties. The best first option is to avoid a specific number if you do not have one. Tell the media that you will share a number when investigators have determined one. However, if specific numbers are already in the air, remember that it is less damaging, for example, to project 100,000 customers affected and then report later that only 50,000 were involved. Starting low and revising upwards leads people to think that the number could continue to escalate. It seems as if you are an unreliable source.

- **Tell the truth**. It always comes out in the end. It is better to take some short-term heat than be later accused of a cover-up or other unflattering activity.

While external and internal communications may be handled by different teams within the organization, the messages should be consistent and integrated. “Official” channels are rarely the only one used and rumors will quickly fill an information void. Given the preponderance of social media one must assume that almost everyone can see almost everything in almost real time: A single tweet from a frustrated employee may be seen by a journalist or blogger. Intrepid reporters will dial number after number remotely close to your main telephone contact in hopes of finding someone to make a statement, so ensure that all employees know to forward them to your designated spokespeople. A bragging “black hat” intruder may even launch the story. A communications-centric exercise can help reveal vulnerabilities and opportunities, build relationships across organizational boundaries, and help develop necessary skills.

Cultivate a Proactive Response Team: Mitigate the Ever-evolving Range of Risks

One of the more fruitful exercises in which we’ve engaged is to ask people at different levels and areas of the organization what “keeps them awake at night”—and what they are doing about it. These conversations can reveal risks that never occurred to risk professionals just as those on the front lines may not perceive the macro-threats revealed through the analyses of risk experts. The operative outlook is that “no one has all of the answers, yet anyone may have part of it.” An inquisitive mindset keeps everyone looking forward to detect the faint signals of crises yet to come.

When adversity strikes, the crisis management team springs into action. The leader can focus and guide their activity using the POP-DOC Loop to establish an efficient “battle rhythm” both personally and for the team. POP-DOC builds on Boyd’s well-known OODA Loop—Observe, Orient, Decide, and Act—used to train fighter pilots worldwide. POP-DOC maps similar optimal cognitive processes along a figure-8 infinity loop for crisis leaders.

POP is the thinking side of the equation. It's three steps are: Perceive—gather a wide array of data on what is happening. Orient—look for patterns that give meaning and significance to the data. Predict—patterns repeat, giving clues as to what will happen next.

The DOC side of loop turns thinking into action. Decide—based on predictions along with assigned priorities and probabilities, decisions are made. Operationalize—to carry out decisions, people need sufficient resources including staff, materiel, and time. Communicate—Ensure that all relevant stakeholders know your course of action and their role in it.

Traversing the POP-DOC Loop, sometimes in minutes and at others using it as a template for team function, helps the leader maintain focus and keep the response moving. The certain, linear steps of POP-DOC help minimize distraction and keep the leader and team looking forward.

CONCLUSION: IT'S ALL ABOUT REPUTATION

Crises happen every day. Some of the largest private and public sector organizations have been hit despite spending enormous sums and employing talented people for mitigation and protection. As noted above, threats are evolving at a dizzying pace. Thus, you may not be able to prevent a breach just as banks cannot prevent every stick-up. What you can prevent, however, is the second crisis of a botched response. This is where your company faces its greatest reputational risk.

Reputation matters. As investor Warren Buffet famously said, “Lose money for the firm, and I will be understanding. Lose a shred of reputation for the firm, and I will be ruthless.” If your organization responds as a sure-footed team that attends to the concerns of stakeholders, you will retain their confidence. If not they, like Buffett, will be ruthless. You stand to lose customers, employees, and perhaps investors. Executives may lose their jobs. Getting a response right avoids unnecessary pain.

Each of the steps outlined above helps create a true leadership perspective on preparedness for and response to a major incident that can keep you focused and productive. They help inform a broad view that incorporates the concerns and needs of the full range of stakeholders. Crisis managers must focus on the “now” of an incident. Crisis leaders are thinking about the future and why people should follow them through difficult times—and beyond. It requires a combination of perseverance and resilience. The concepts and tools above will help leaders and their teams cope with the human dimensions of high stakes, high stress situations, avoid common pitfalls inherent in complex situations, and foster robust connectivity with other functions and operations across the enterprise during a significant crisis response.

ACKNOWLEDGEMENTS

We thank Mark Sutton, CISO of Bain Capital, Thomas Samuel, CISO of KKR, and USAF Col. (ret) Ron Banks, for their comments on and review of this white paper.

For more on any of the concepts, tool, and techniques in this paper, see *You're It: Crisis, Change, and How to Lead When it Matters Most* (PublicAffairs, 2019) by Leonard J. Marcus, Eric J. McNutly, Joseph M. Henderson, and Barry C. Dorn.