WHAT BOARDS AND EXECUTIVES CAN LEARN FROM GOVERNMENT CRISIS MANAGEMENT

Companies in a crisis face growing demands to demonstrate transparency, responsiveness and accountability

Although companies don't often face life or death threats, they do confront situations that require quick and well-managed responses: cyber-hacks of corporate trade secrets, accounting fraud and allegations of sexual misconduct, to name a few. For company leaders facing a crisis, lessons learned from government can serve as both a cautionary tale and a best practice.

Today - at a time when the well-being of multinational companies can elevate or depress entire economies - corporate executives and boards of directors are facing the same intense pressure the public places on government leaders in Washington, DC: respond to the crisis with transparency, responsiveness and accountability.

The public demands that leaders tell people about the problem early on, tell them how you're going to solve it and demonstrate how it will never happen again. Doing this is a simple formula for crisis management, but it can be a near-impossible one to follow when the pressure is on.

The US Department of Homeland Security (DHS) sits at the epicenter of potential crises. As its former chief of staff, I had the privilege (and daily demands) of being part of a full-time crisis response team. Whether confronting cyber-hacks of federal systems, terrorist attacks or the theft of classified or other sensitive information, we relied on several key steps that helped us respond in meaningful and efficient ways. Lessons learned from these scenarios can work for companies navigating their own challenges.

1) Recognize that you're in a crisis

The government's response to Hurricane Katrina is an oft-cited example of failing to respond to a crisis quickly enough – particularly for not sufficiently recognizing the gravity of the situation and the swiftness with which the crisis was unfolding.

For companies, the ability to anticipate the potential consequences of a challenge in the early days of what may be a seismic crisis is key. To do this, you need the right experience in your senior leadership team. That means having individuals who have lived through crises so they can help you recognize one as it emerges.

Sometimes this role may be taken by the head of corporate or external affairs, or a chief compliance officer. Large companies may have a separate consigliere-like position reporting directly to the CEO. At other companies, this role may be filled by the general counsel or another C-suite executive who has lived through crises. Wherever it sits, that position should help the executive team and board recognize the warning signs of a crisis and adhere to the golden rule of crisis management: don't make it worse (which is surprisingly easy to do).

The consequences of failing to recognize early enough that you're in a crisis can be disastrous, particularly when considering potential litigation. Take, for example, a scenario where a cyber-security breach occurs. Before a company understands it is in a crisis, members of the technology or HR team may be conducting their own investigations into the matter – and in doing so creating an archive of discoverable emails and evidence.

Also, the cyber-actors may still be in the system accessing and removing increasingly sensitive information. Or executives may be trading company stock while potentially armed with non-public information that a breach has occurred.

That is why having the right team in place early on is key: to protect privilege and security, to address the problem and mitigate further harm and to launch a host of other remedial mechanisms that will become critical down the line.

2) Form a team

Once you're in, or imminently close to, a crisis, quickly form an internal crisis-response team. Identify a point person with authority and accountability and set a battle rhythm. There is no substitute for empowering a single action officer to make all aspects of the crisis his or hers. There are likely countless other important issues facing the company and the business of large organizations must go on; this model allows a senior accountable official to own every detail, fact and response, in close coordination with corporate leadership.

The team should include representatives from all relevant business units and functions – including operations, public affairs, government affairs and legal – and it should be creative. Solutions to your crisis will not be singular. They will require a range of tactics, including operational fixes, organizational changes and public engagement that are all interconnected. A cross-disciplinary team with a mandate to think creatively is a powerful tool to mitigate a crisis.

This approach should not be confused with passing along a crisis to a lieutenant and forgetting it. On the contrary, corporate leadership needs regular updates and meetings to prepare for key decisions as the crisis-response team marches forward. But organizations still need to function, and this approach allows just that.

As the concern about Ebola spread in 2014, DHS was ground-zero for safeguarding the flying public. To do so, we formed a crisis-response team with all relevant agency functions represented, conducting daily (sometimes twice-daily) check-ins, completing action items, reporting to the DHS secretary and obtaining key guidance when necessary. The team approach encouraged and facilitated the sharing of ideas and the free flow of information, and ensured actions were taken quickly and correctly.

One Saturday afternoon in the early days of the crisis I received a call indicating that a passenger who had originated in West Africa had become very ill in flight. The plane was due to land in the US shortly and dozens of

novel and complicated questions immediately needed answers: should we allow the plane to land? What if the ill passenger resisted being isolated? Would we allow the other passengers on the plane to leave the airport for fear they may have contracted the illness? Answering these and many other challenging questions of first impression was made somewhat easier with an established and broadly represented crisis-response team in place.

3) Develop a plan

The next step is to develop a plan and roll it out for the world to see. Whether the audience is your shareholders, consumers, Congress, regulators or some other stakeholder, organizations in crisis and their leaders need to reassure everyone that they get it and have a path forward to resolve the issue and make sure it never happens again. There is no better way to show competence in this regard than by having a plan and making key parts of it public.

Of course, this presupposes a key element to crisis management: acceptance of responsibility. The public can be remarkably forgiving when it feels you are transparent, but the patience to forgive erodes quickly under a cloud of distrust. Accepting responsibility is one of the more challenging decisions a board and executive team typically face, particularly in scenarios where the full facts and scope of liability remain unknown.

In the early stages, it may be impossible to place responsibility for the cause of the crisis on any one set of shoulders, but it is often possible to accept responsibility for the outcome and for preventing the next one. A company can communicate a plan for getting to the bottom of the facts, creating better safeguards for the future and taking active and affirmative measures to ensure the crisis is remedied.

A plan can have many components, depending on the particular challenge. Whether it has five points or 10, the primary requirement is that it be clear, relayed in plain language and demonstrate accountability. Some of the steps may include an independent internal investigation (often conducted under privilege by a law firm), a follow-on report, personnel changes to address systemic problems, and concrete measures to plug any gaps that may have contributed to the problem.

For example, after breaches of White House security and extraordinary follow-on scrutiny of the Secret Service and DHS, its parent agency, we commissioned a blue-ribbon, bipartisan group of unimpeachable experts to study the security challenges and report to the DHS secretary on how best to correct the problems. With such a report came the expectation that the findings would be shared, which is important. Sharing key findings can and should be done while still protecting certain confidential information.

Similarly, the recommendations should be made public to the greatest extent possible, particularly in high-profile crises. In our case, doing so helped convince the public and Congress that we were taking the issue seriously and had a real plan moving forward. The plan and its publicity provided the added benefit of creating some distance from the crisis, which gave us time to address the problems while not in a constant state of siege.

Members of the team are human, which means there won't necessarily be consensus for every action. That's OK. No crisis-response team will succeed if it requires absolute consensus before moving forward. Broad input and inclusion is critical, but give up on reaching a consensus: in the middle of a crisis, it will often be unattainable. The team is in place to address difficult questions and make hard decisions and, when appropriate, to tee up a particularly sensitive issue for the corporate leaders whose job it is to make tough decisions.

4) Understand your reporting obligations

Depending on the nature of the company and crisis, an organization may be required to make some degree of disclosure. This underscores the importance of having broad representation on your crisis-response team. In particular, lawyers on the team will be working from the beginning of the crisis

to determine what legal obligations there may be, which may include notifications to shareholders, consumers or regulators, and reporting them to the action-officer for discussion among corporate leadership.

Companies should also consider what voluntary disclosures or public statements they should make, even when they are not required to do so. For example, does it make sense to disclose a potential foreign bribery allegation to the government, even though that may not be mandated? Should you make a public disclosure about cyber-security breach where no disclosure duty exists , or limit it to only what may be required?

There is no easy answer to this, but it demands consideration. On the one hand, depending on the size of the problem, it may never come to light but for your making it public. On the other hand, failure to report can ruin your company's credibility, or lead to criminal and civil penalties. For government investigators watching your company and retracing the decisions made by executives and boards in the moment, sunshine and transparency go a very long way.

This strategy can also provide some public relations advantage when the circumstances are right. It provides the added benefit of minimizing the chance of a drip, drip, drip crisis, which is the worst kind. Getting all the facts out at once demonstrates transparency and acceptance of responsibility, two key elements to quickly moving beyond a crisis.

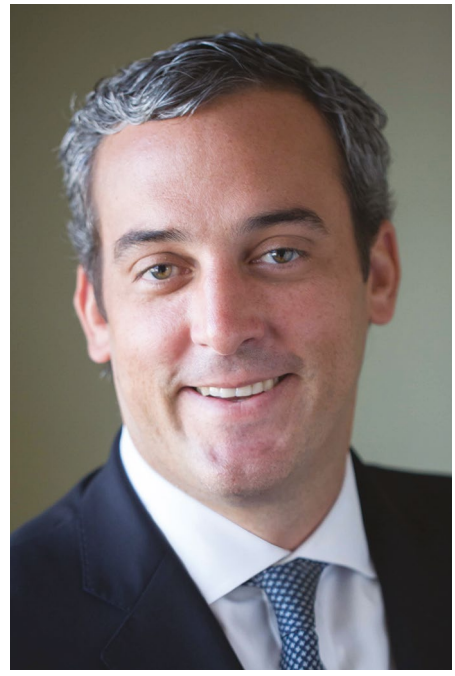
Not coincidentally, these are the same two factors government regulators and investigators will be looking to see when they consider whether and how to pursue actions against you. The approach also maximizes the chance to make the crisis just a one-day story.

5) Learn lessons

Finally, learn from the crisis, share that learning and train your employees. Once through a crisis, the natural reaction is to breathe a sigh of relief and move on to the next issue, particularly in a fast-paced environment. But leaders should stop and think about how they can use what happened and what they learned to make systemic improvements to the organization.

After-action reports are often key in this regard. At DHS, a relatively young agency born out of the 9/11 terrorist attacks, we made a point of learning from each crisis to improve the management of the agency and the processes and procedures throughout the organization.

If you're helping to lead a large organization, you will inevitably face crises at varying levels – so have a game plan. Practice that plan. Learn from the mistakes of the past. Doing so demonstrates that you're constantly striving to do better, and better prepares you and your team to deal with the next 3:00 am call.



Paul Rosen is a partner with Crowell & Moring. He most recently served as chief of staff for DHS and previously worked as a federal prosecutor.