2018 CRISIS MANAGEMENT BENCHMARKING REPORT

Understanding Companies' Preparedness and Best Practices for Closing the Crisis Management Gap

MORRISON FOERSTER

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

EXECUTIVE SUMMARY

On behalf of Morrison & Foerster and Ethisphere, we are pleased to present this global Crisis Management Benchmarking Report. The report is designed to give corporate legal departments insights into current trends involving crisis management professionals and teams around the world and to highlight best practices for crisis planning, table top exercises, and more.

The survey that forms the basis of this report was conducted in the spring of 2018 to a global audience and included questions about crisis management programs, how companies prepare their teams, and the ways that companies employ outside counsel. We collected approximately 250 responses from senior executives in ethics, compliance, legal, communications, and risk functions from both public and private companies and non-profits across the globe.

The data from this survey, combined with interviews from large, multinational companies with sophisticated legal, ethics, and compliance programs, as well as from Morrison & Foerster partners with extensive experience in various domains of corporate crisis management, informs these findings and recommendations. We are grateful for the contributions of the diverse professionals and organizations who participated in the survey and shared their insights with us.

Some key findings from our study include:

Cyber breaches remain a key area of concern for crisis management teams

The crisis area that companies are most concerned about is a potential cyber breach. This is a reasonable concern as our world continues to be increasingly digitally interconnected, and more and more devices are WiFi or Internet enabled (the "Internet of Things"). The next most commonly included crisis event was "workplace violence or harassment" (reflecting additional steps being taken by companies to address these issues in the #MeToo era).

The majority of companies are, at best, only "somewhat confident" of their crisis management plans

Despite widespread understanding and adoption of crisis management plans, 56% of respondents suggested they were only "somewhat confident" in those plans. Add to that the 9.9% of respondents who selected they were "minimally confident," and a clear majority of companies do not feel as prepared as they should be to respond to an unexpected crisis event.

Having a plan is a good first step, but benchmarking and training is key

Companies suggested they were very confident in their crisis management plans when benchmarking against best practices on a regular basis (87% of companies that are "very confident" in their plans benchmark their plans), when conducting drills on key risk areas at least once a year (64%), and when having a formal, documented crisis management team (93%). This suggests, not unlike how the best companies approach compliance and ethics preparedness, ongoing review and preparation is critical in having an effective response to an unexpected crisis event.

Outside counsel can be a valuable asset in crisis response plans

Finally, outside counsel are also an excellent resource in supporting companies' crisis management plans and responses. Outside counsel, in addition to traditional roles, such as general strategizing and planning, can play a key role for advanced planning with communications firms, reviewing contractual provisions, and also helping advise on interactions with relevant regulators for a given crisis.

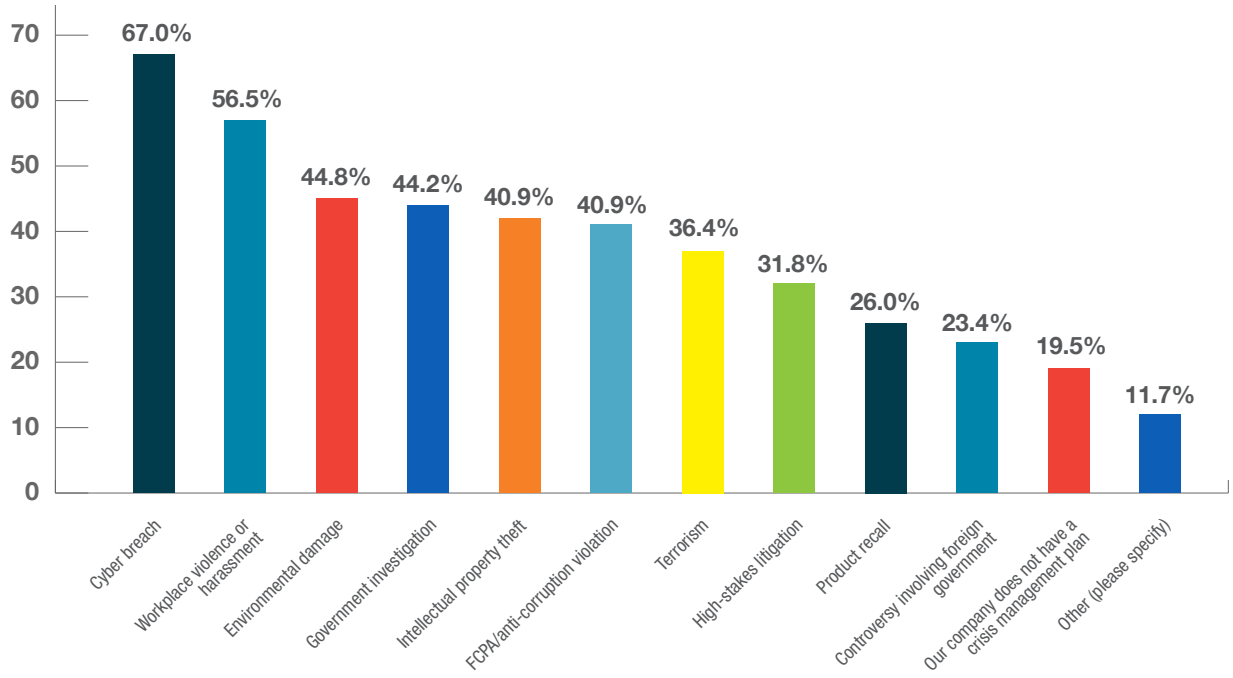
TABLE OF CONTENTS

SECTION ONE:

KINDS OF EVENTS INCLUDED IN CRISIS MANAGEMENT PLANS

One of the areas our survey explored in depth involved the types of events companies included in their crisis management plans. The most common response was "cyber breach," with 67% of respondents answering that they had plans that addressed such an event. The next most commonly included crisis events were "workplace violence or harassment" (reflecting additional steps being taken by companies to address these issues in the #MeToo era) (56.5%), followed by events relating to a government investigation (44.2%) and environmental damage (44.8%). Beyond those, tied at 5th and 6th, were preparations for an anti-corruption violation (40.9%) and an IP (Intellectual Property) theft event (40.9%), followed by terrorism (36.4%), high stakes litigation (31.8%), and product recall (26%).

WHICH POTENTIAL ISSUES DOES YOUR CRISIS MANAGEMENT PLAN ADDRESS? PLEASE SELECT AND APPLY.



That cyber and sexual harassment were the most commonly cited answers is expected, as both types of events are highly visible and front of mind for corporate executives. Understandably, when executives try to anticipate and plan for a "crisis," their thinking is informed by what could become a major reputational crisis. Given the potential risks these types of events pose, it is critical that organizations of all sizes assess their level of preparedness in these areas and ensure that their crisis management plans adequately address them.

At the same time, however, there are plenty of crises that do not necessarily involve reputation for which a crisis management plan can, nevertheless, also prove invaluable. These areas should not be overlooked.

As Todd Cioni, Vice President and Chief Compliance and Ethics Officer at CareFirst, notes "your plan needs to be able to take into consideration everything from a water main break making your building inaccessible to a data breach. The elements and stakeholders will be different, but the fundamental components will be the same: know who is doing what, who needs to know what when, and who is responsible for getting information to those parties." Cioni goes on to note that companies looking at their crisis planning process should:

OVER DOCUMENT, SINCE YOU CANNOT PREPARE FOR THE PRESSURE INVOLVED IN A REAL CRISIS;

CONSIDER THE SPEED TO RESPONSE IN YOUR PLANNING AND APPRECIATE THE ABILITY OF A CRISIS TO GROW OR BE CONTAINED WITHIN HOURS; AND

PLAN ON HOW YOU ARE GOING TO ACTUALLY REACH PEOPLE IF COMPANY SYSTEMS OR FACILITIES ARE INACCESSIBLE. WHAT OFF-BAND COMMUNICATION OPTIONS DO YOU HAVE?

David Newman, of Morrison & Foerster's Global Risk & Crisis Management and National Security practices, highlighted the importance of ensuring that the response plan reflects input from all relevant components of an organization and is tested with the actual participants who would be called upon to use it through tabletop exercises and other drills. "Don't prepare in silos. Consider not just preparation within workstreams but true cross-functional planning; part of the purpose of a good tabletop exercise is to give people the experience of working through challenging scenarios and elements of the response. To be able to go fast and also be effective, you have to have practiced."

And, consider the tabletop exercises as something more than just a drill; Christine Wong, a partner in Morrison & Foerster's Investigations and White Collar Defense practice and formerly head of international compliance at a major multinational company, used the drills in which she participated while in house as an opportunity to build relationships between members of a crisis response team. "Design them so people across the business have a chance to talk and get to know each other. That makes it more likely that in the thick of a crisis, information will flow the way it is designed."

Although over half of companies in the survey responded that their plans included scenarios involving sexual harassment allegations, that number appears set to rise. Given the increased prominence of such issues, every company should plan for how they would effectively respond to allegations raising such issues, including allegations involving employees, especially senior executives, or to allegations that reflect poorly on a company's culture more broadly. In addition, those who have plans that already address such events would do well to consider whether they are in need of enhancements. The chief compliance officer of a major global retailer explained that the company has incorporated a crisis component into their root cause analysis following significant investigations, using findings and lessons learned from the investigation to probe whether changes should be made to their crisis plan.

Another company, a Fortune 200, global manufacturing organization, noted that they review their crisis plans in conjunction with their annual enterprise risk management process, to make certain that they are matching their plans to their evolving risks. In the case of sexual harassment-related crises, while companies are

responding to the increased visibility these issues are currently receiving, they are increasingly considering not just the legal implications of the issue but also the cultural component. As Carrie Cohen, Co-Chair of the Workplace Misconduct Taskforce + Investigations and White Collar Defense partner at Morrison & Foerster, noted, "companies are looking beyond the law to ask how the behavior may affect the culture, and boards are becoming involved and looking to understand the risk."

This senior-level focus on the issue allows companies to include directors in conversations around crisis management; as one retail company we spoke to following our survey noted, they are now doing annual reviews of crisis planning at the board level so that all directors understand their decision-making roles and responsibilities.

One kind of crisis that presents a modern and unique challenge, and which approximately 26% of respondents planned for, is a product recall. While product recalls have been a longstanding crisis area for companies, we wanted to specifically address this area of risk given the way that increasingly connected devices – the Internet of Things – plays into how a recall can be effectively executed. This is one area where many companies are currently reactive, but preparing and planning for a recall is essential. While recalls may seem rare to the layperson, if you consider all of the potential permutations of a repair or recall, they are not.

Erin Bosman, chair of Morrison & Foerster's Product Liability and Counseling practice, notes that a good product recall plan is similar to a general crisis plan, but she encourages companies to think about "two different stakeholder groups – those in the company who will respond, and those outside the company who will be impacted." In the past, product recalls were strictly the purview of the manufacturer and the user, but with the proliferation of connected devices that model needs to be reconsidered.

Bosman recommends that companies consider how device connectivity might affect their customer interactions. "The number of connected devices has grown tremendously in the past several years. So has the importance of understanding how connected devices interact with their users and the ability to reach a consumer. Consider a connected thermostat. How would you notify your customers? Sending mail is no longer the leading practice. Instead, consider how you'd reach out through your app. What about software or firmware patches? Who can get the messaging pushed out? It's critically important to know who does those things, and what approvals you might need to get. Assume that the platforms you've used to promote the product are the same ones you will need to use to tell your customers about a recall."

Cyber Dominates in Planning, but Not Preparedness

One of the major findings to emerge from our crisis response survey was the degree to which companies' crisis response plans continue to be focused on cybersecurity concerns. It's easy to see why this would be the case: the list of multinational companies whose reputations have been tarnished by a cyber breach or other adverse event is long and ever-growing. One study of 24 recent cyber breaches found that reports of a breach are typically accompanied by a fall in stock price in the short-term and sustained, slower growth in the long-term.[1]

John Carlin, Chair of Morrison & Foerster's Global Risk and Crisis Management practice group and Co-Chair of the National Security practice group, emphasizes that the responsibility for mitigating cyber risks has changed. "It used to be this is the domain of the technologists, but now people understand there's no technical fix and we need a culture of compliance where cyber security and risk mitigation is everyone's responsibility. The other change has been to include this fully within risk management, with a focus on resiliency. Ask yourself: what am I most worried about? Start there, and think about how you'll get back up." Emphasizing the importance of speed and coordination in responding to cyber events, Carlin notes that an incident response plan has to include all key members of the company and has to be tested with the relevant participants. "That level of practice makes the critical difference between unpleasant and catastrophic."

Bischoff, Paul. "Analysis: How Data Breaches Affect Stock Market Share Prices." Comparitech. https://www.comparitech.com/blog/information-security/data-breach-share-price/

PREPARATION ADVICE

Before an IP issue arises, Eric Akira Tate, Co-Chair of Morrison & Foerster's Global Employment and Labor Group, outlines some basic protective measures companies can take to help mitigate the chance of IP theft:

1) It may conflict with BYOD preferences, but only allow use of company-issued devices and sources of data, and periodically monitor compliance with this rule;

2) Review with employees during on-boarding and periodically during employment the company's policies regarding confidential and trade secret information and its use and non-disclosure, and have employees periodically reaffirm in writing their understanding of these policies;

3) Ensure return of all company-issued devices and access information for sources of data (e.g., cloud accounts) from departing employees;

4) For any disgruntled employee who had access to company confidential information and trade secrets, consider whether to review his/her activity and/or retain that former employee's company-issued devices and sources of data (as opposed to erasing and repurposing for another employee);

5) Send a letter reminding the employee of his/her obligations to return and maintain the confidentiality of any company confidential information or trade secrets; and

6) If you find evidence of illegal activity, consider initiating legal (civil and criminal as appropriate) action promptly.

In keeping with the emphasis on potential cyber breaches, nearly half of respondents (47.5%) said their Chief Information Security Officer (CISO) plays an active role in crisis response. This makes sense, as it is one of the roles necessary to respond to a cyber crisis. Carlin also notes four other critical parties to include in a cyber-related crisis response plan: your outside counsel, your crisis PR firm, a forensic firm, and the vendors necessary to meet the needs of customers and to respond to the underlying incident.

A further 15% of companies actually go so far as to put the CISO in charge of crisis response for all types of crises by default. While having the CISO and their team involved in crisis response to a cyber event is a model that is often used, putting a CISO in charge of all crisis response – even events unrelated to cyber – may not adequately take into account the myriad forms of crises a company might face and resulting challenges. While the CISO's office will be quite helpful in formulating a response to a data breach, they would be much less informed concerning response to a crisis brought on by a natural disaster, for example, or an active shooter.

Tellingly, despite the fact that a majority of companies expressed cyber breach as their number one concern, most companies did not actually feel prepared in responding to a cyber breach. When asked which sort of crisis they felt least prepared for, nearly a fifth of companies identified "cyber breach" as their chief concern, behind only terrorism. As Carlin shared, the ever-evolving nature of cyberattacks puts even more of an emphasis on preparations in two areas: making sure your employees and third parties remain aware of the company's protocols around cyber protection and follow them and making sure your drills evolve with the nature of attacks. "You cannot drill and then put your plan on a shelf," he notes.

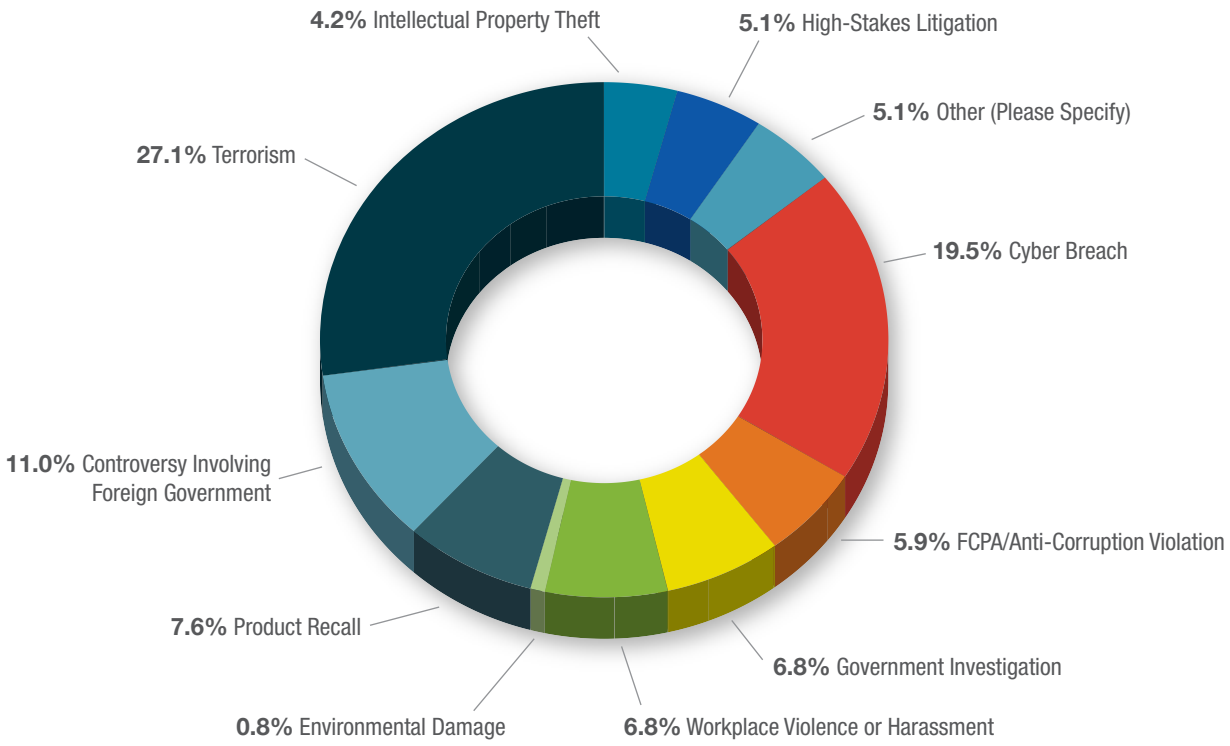
A tangential and sometimes overlapping area of risk to cyber breaches for companies is intellectual property theft, which can come in the form of remote cyber attacks or employees physically sharing sensitive information with outside parties. This can come from a direct, intentional act of malice by a rogue employee or happen unintentionally when an individual inadvertently leaves sensitive information unsecured against a company's policies. Regardless of how the IP loss arises, a company's response should be swift says Eric Akira Tate, Co-Chair of Morrison & Foerster's Global Employment and Labor Group.

"The best defense is always to limit the disclosure of IP as much as possible in the first place," according to Tate. "Unfortunately, if a once trusted employee decides for whatever reason to go rogue, there is only so much a company can do to stop it, and the speed of the employer's response to a breach becomes more important."

This is especially true in high-stakes litigation, for example, when a competitor has hired an employee who has critical IP.

"If a company hires an employee from a competitor and learns that its new employee may have retained the competitor's IP, it should confirm the extent of any disclosure of such IP elsewhere in the company, put in place a process to prevent and/or limit any further disclosures, as the case may be," Tate says. "In doing so, a number of considerations, including but not limited to who participates in the process and how, and what to do going forward with the new hire, will be involved and determined on a case-by-case basis. The little and big steps in this scenario are critical to get right."

WHICH CRISIS DO YOU FEEL LEAST PREPARED FOR?



A More General View of Crisis Response Planning?

The complexity of the issues that can arise from the areas identified as those in which companies are least prepared (cyber breach, terrorism, controversy involving foreign governments, etc.) suggest that having a crisis management plan on paper is only the first step in what must be a much broader effort at crisis preparedness.

Although it can be tempting to build specific crisis responses to every foreseeable issue, the truth is that no plan can or should cover every crisis scenario; and, when a crisis does hit, it may occur in a way that would not have been on anybody's radar at all. Given that fact, the most important element of a crisis response plan is that it be adaptable to a broad set of circumstances, with clearly-articulated steps and involvement for all company stakeholders.

Fortunately, a well-planned-out crisis response plan should work for a variety of issues, whether it is focused on an anti-corruption issue, a competition law issue, or another regulatory risk. The first step is to honestly assess risk, and the quality of the compliance program currently in place, including reporting lines that are utilized and trusted around the globe. As Cohen notes, "look inward first. Do the self-examination needed to identify the threat. Do the sophisticated risk analysis to identify risks, and be sure to understand the business. It is easy to overlook a risk or a regulator on the local level, such as someone active in your industry at the state level."

Ruti Smithline, co-head of Morrison & Foerster's Investigations & White Collar Defense Group, notes "crisis management is really part of proactive preparation – how to address a crisis is really about how prepared you are to manage risk."

Preparing for key risks when crisis planning and making sure you understand your

regulators is a critical step, says John Smith, Co-Chair of Morrison & Foerster's National Security Group and former OFAC director. "Remember that even though platforms and technologies have evolved, the regulations still apply."

Several of the companies who participated in the survey noted how closely tied their compliance programs are to their crisis planning processes. Their training and communications efforts influenced how they prepped to manage a crisis, and vice versa. That reflects a broader thinking around training, which Wong notes as "training as you go, providing off the moment information when it is most important."

This is also applicable to the way companies conduct investigations. Cohen agrees and notes the "who/what/when/where/how skill set that counsel brings to the table provides the necessary background to respond to a crisis." This includes how a company might respond to a request for information from a regulator. Smithline notes that the evolution from the written letter to email and now to apps and chat technology puts even more importance on training employees on the dos and donts of communications.

Lisa Phelan, a partner of Morrison and Foerster's Global Antitrust Law and Investigations & White Collar Defense practice, also notes that as part of the planning process, companies should consider adequately preparing executives for regulatory interest, including "knock and talk" interviews. For example, consider whether a dawn raid plan needs to become a part of the compliance program , including knowing which employees would be affected by such an unplanned visit by investigators and providing training to ensure all employees respond in a way that meets the expectations of the company, while being consistent with all federal and local laws. As dawn raids are a common tool for regulators around the world, it is often helpful to engage outside counsel with experience dealing with global regulatory agencies to help your company properly plan and train for such an event.

Moving beyond crises that involve negative media attention, other issues and emergencies could also be addressed by a flexible plan. Natural disasters can impact companies in a variety of ways, either through harm to company assets or even to employees' homes and lives. Depending on the nature of a business, supply chains of key products may also be impacted by disasters, even in regions or countries where a company does not have direct operations. There may also be value in a crisis plan that would address various forms of leadership and governance crises, including events such as the sudden death of the CEO, that can create intense challenges for the continuation of the business. An adaptive, generic crisis management plan could help a company respond quickly to any of the above situations.

Addressing Risk Created by Third Parties in Your Crisis Planning

One growing area of crisis management for many organizations is third-party-created risk. As Cioni notes, "in our increasingly interconnected world, an issue at one company might quickly become an issue at yours, so it is vital you consider that in your planning process and open lines of communication with your key third parties."

Both Smith and Smithline agree, as compliance expectations for a variety of risk areas become increasingly embedded in the due diligence process, and not just upon initial selection but also with updated assessments over time. Once again, always tailor this kind of program to your risks, but the more holistic your third-party program can be, the more prepared you can be for an issue. Consider too the third parties of any entity you might be acquiring and how those third parties are selected. Understand any ongoing monitoring and the quality of the program, and make sure both are up to company standards for the risks they present. As Wong notes, if the root of a crisis is a key third party, then the more you can communicate between compliance teams, the better.

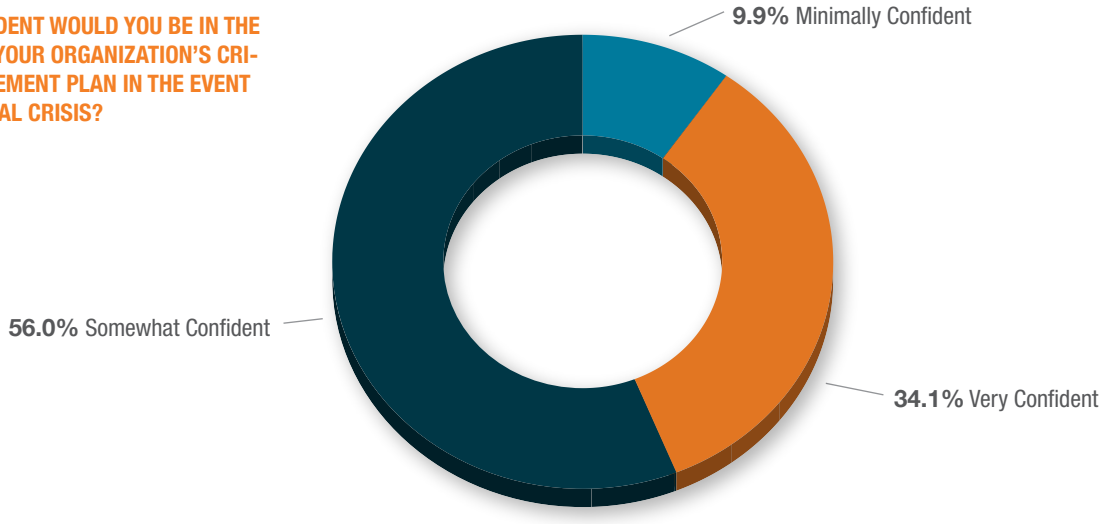
SECTION TWO:

BOOSTING CONFIDENCE IN CRISIS RESPONSE

Crisis of Confidence in Crisis Management?

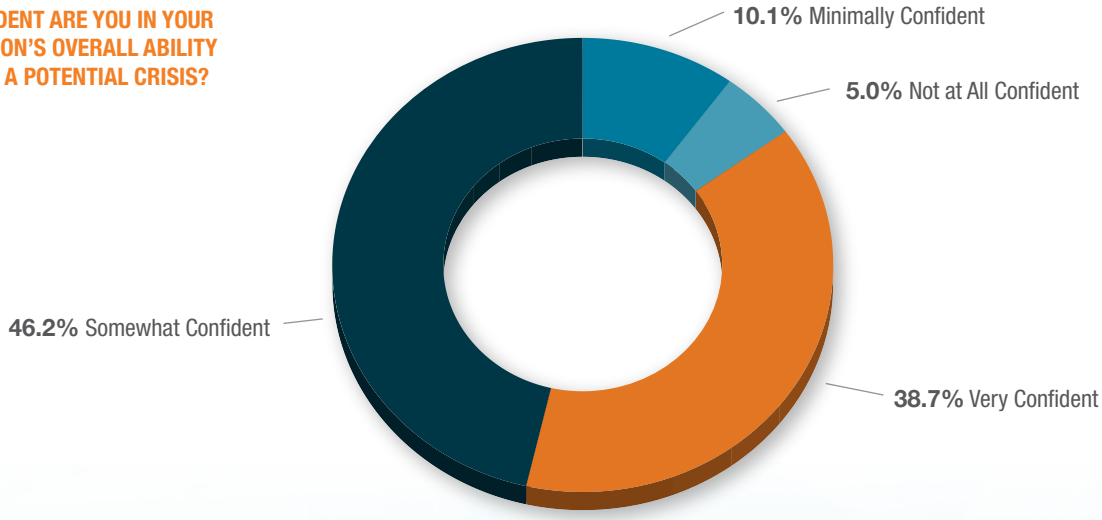
Another interesting set of data points to emerge from the survey revolved around companies' confidence in their crisis management plans and execution. The majority of respondents (56%) were only "somewhat confident" in the utility of their organizations' crisis management plan-in an actual crisis, with 10% actually saying they were "minimally confident" in their plan. Taken together, that means that two-thirds of respondents had misgivings about their organization's plan.

HOW CONFIDENT WOULD YOU BE IN THE UTILITY OF YOUR ORGANIZATION'S CRISIS MANAGEMENT PLAN IN THE EVENT OF AN ACTUAL CRISIS?



In terms of actually executing to manage a crisis, the surveyed organizations felt only minimally better. Slightly less than half (46%) were "somewhat confident" in their ability to actually manage a crisis, 10% were "minimally confident," and 5% of respondents were "not at all confident" that their organizations could manage a crisis.

HOW CONFIDENT ARE YOU IN YOUR ORGANIZATION'S OVERALL ABILITY TO MANAGE A POTENTIAL CRISIS?



Methods to Raise Organizational Confidence

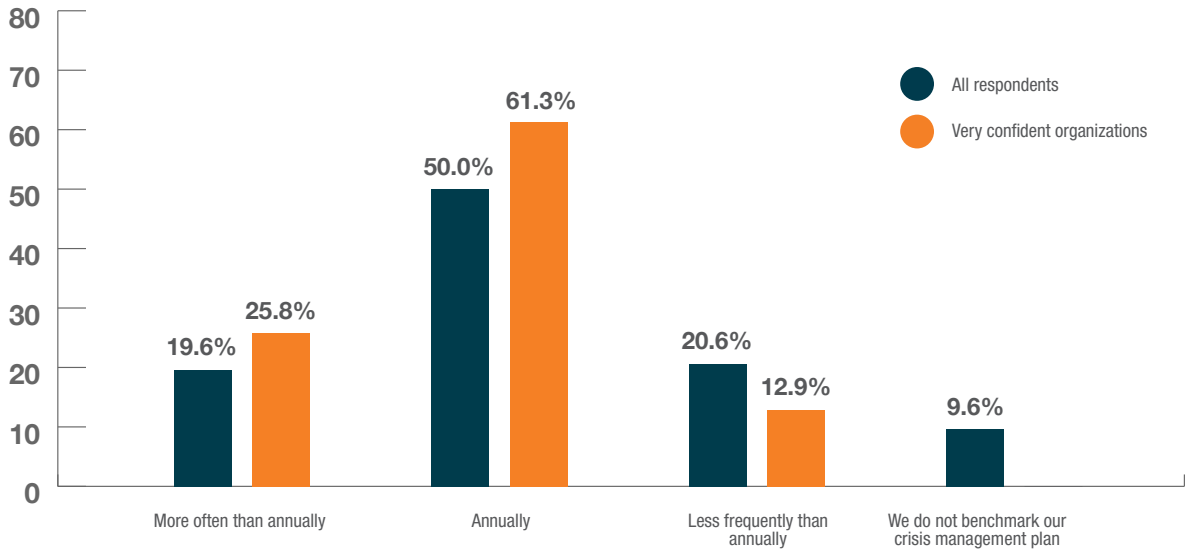
In order to discover what practices might raise confidence in an organization's ability to manage a crisis, we looked at differences between companies who were "very confident" in their crisis management plans, and those who suggested they were minimally or not at all confident.

The bottom line is that companies that regularly update their plans based on best practices in the field and that drill on them with relevant executives and crisis-team members expressed a greater degree of confidence in their level of preparedness.

Pathways to High Confidence:

1) Companies were more likely to say they were very confident in their plans when they benchmarked their crisis management plans at least annually against best practices in prevention and regulatory compliance (87% of those who were very confident, versus 72% of those who were not).

HOW OFTEN DOES YOUR COMPANY BENCHMARK YOUR CRISIS MANAGEMENT PLAN AGAINST BEST PRACTICES?

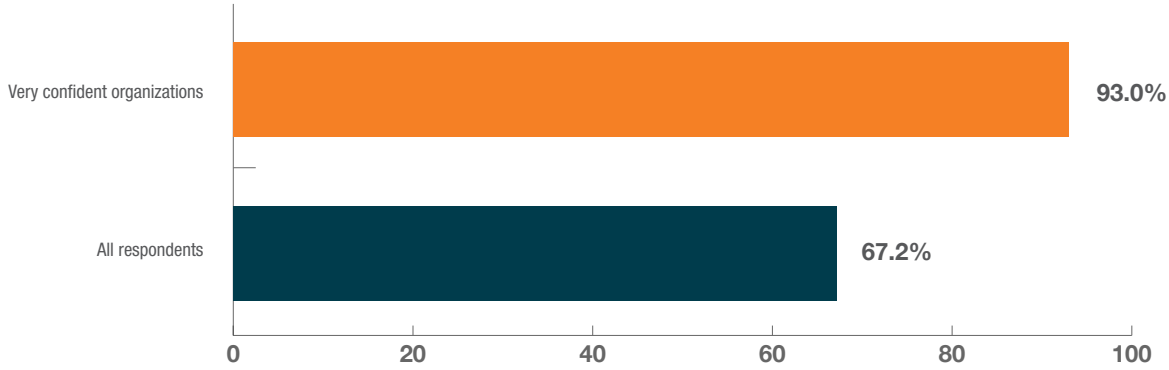


Benchmarking an existing crisis management plan against best practices serves several purposes. Most obviously, it ensures an organization has a chance to review and refresh the plan every year, updating it with new risks. However, it also serves as an ideal chance to re-engage everyone involved in the plan, remind them of their roles, and keep current the relationships and organizational "muscle memory" to react in an actual crisis.

> "companies that regularly update their plans based on best practices in the field and that drill on them with relevant executives and crisis-team members expressed a greater degree of confidence in their level of preparedness."

2) Companies who were very confident in their crisis management plans also tended to have a formal, documented crisis management team (CMT). 93% of "very confident" organizations had one, while only 78% of organizations who selected not at all confident did.

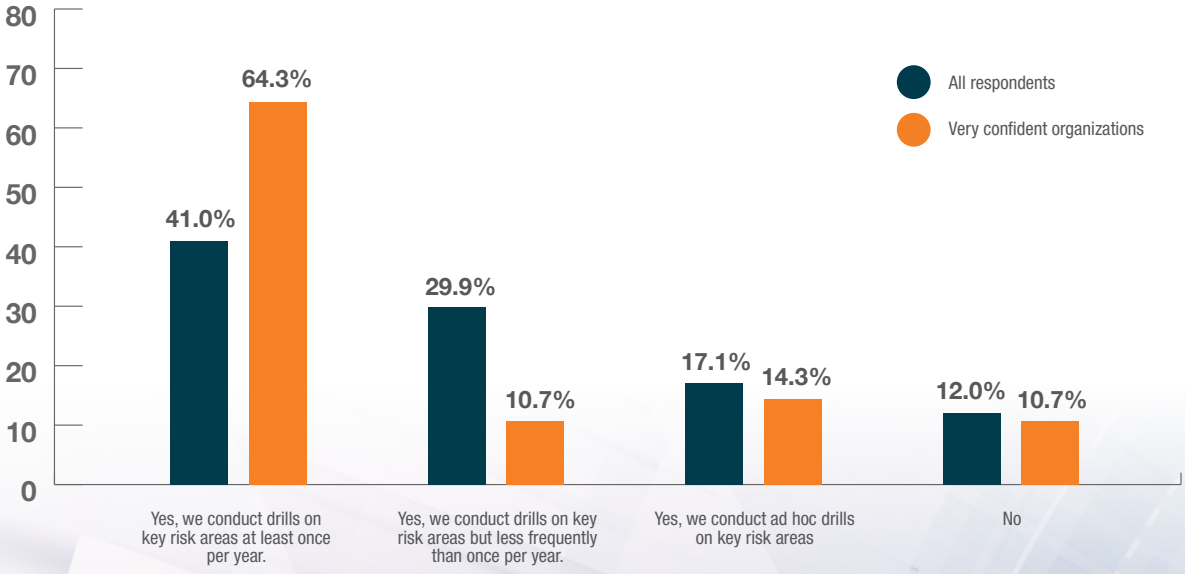
DO YOU HAVE A FORMAL AND DOCUMENTED CRISIS MANAGEMENT TEAM (CMT)?



Identifying a formal crisis management team is another relatively simple step that correlates with increased confidence in the ultimate success of a crisis management plan. That makes sense: having a formal CMT means that all of the right people can be summoned easily if the plan is activated, with roles pre-assigned and potentially rehearsed. And increasingly there is an important role in that process for a broad multifunctional group, including compliance.

3) Nearly two-thirds (64%) of companies who were "very confident" in their crisis management plans conducted drills on key risk areas at least once a year. Only 37% of companies who were less confident did the same.

DOES YOUR ORGANIZATION CONDUCT CRISIS RESPONSE DRILLS ON KEY RISK AREAS?



The practice most correlated with very confident organizations, conducting drills in key risk areas, is also the most time- and labor-intensive. However, it's easy to see why it would improve organizational confidence. After all, it's one thing to have a "paper plan" in place with roles to be played in the event of a crisis, and roles assigned on a formal CMT. However, the only way to know if the plan would work in an actual event is to put it into practice, whether in a real situation or in a well-designed simulation. Periodic table-top exercises and other response drills take time and should be executed thoughtfully. But if done right, they can make a marked contribution to an organization's overall level of preparedness and ensure that their plan will be relevant and useful in the event of an actual crisis.

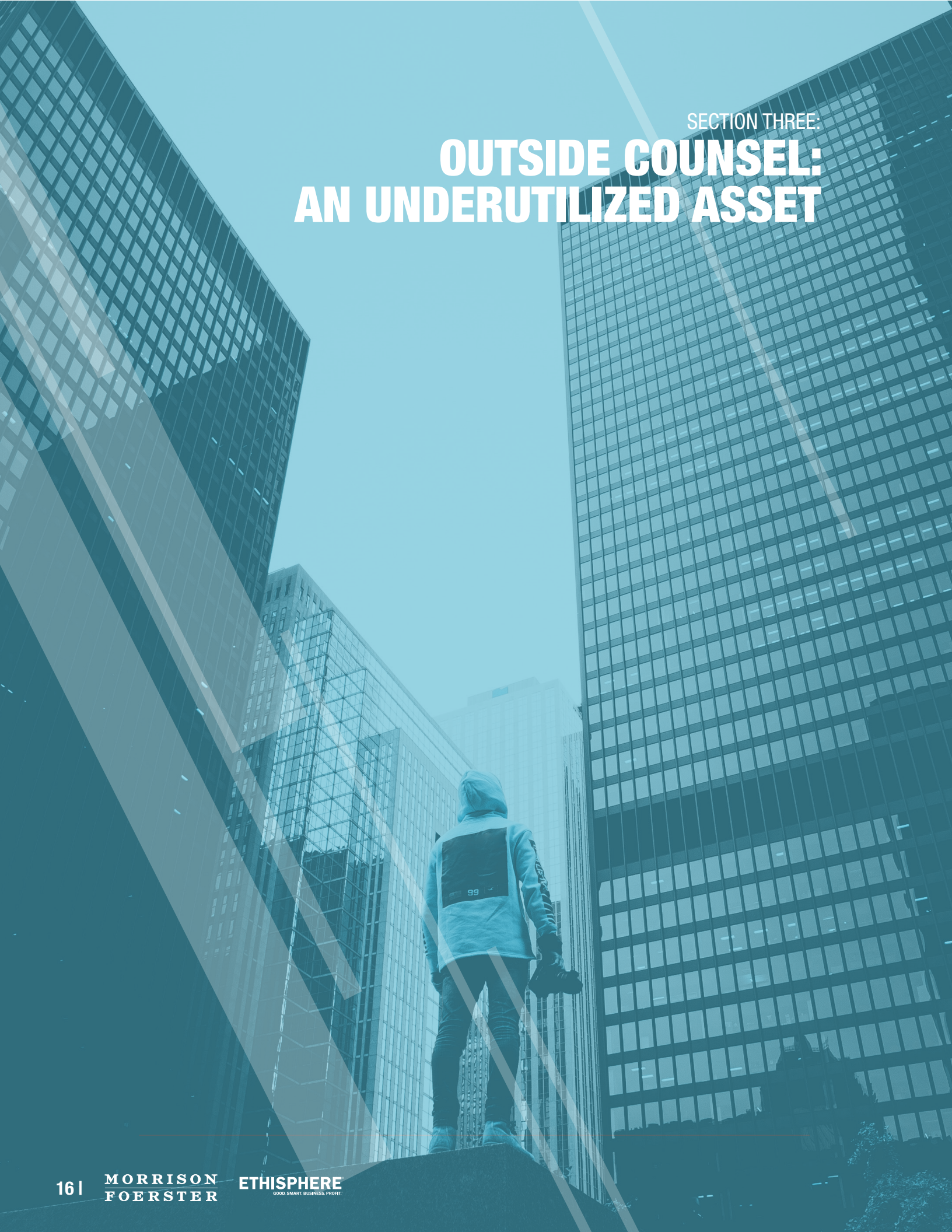
One possible way to drill a crisis management plan that will still effectively engage resources is to run the plan on more "minor" events. Rather than scheduling one simulated drill every quarter, for example, an organization could identify smaller events that, while they may not be existentially threatening to a business, shareholders or other stakeholders, might still be addressed by the CMT and treated as a drill. Determining what constitutes a minor event that can be used as a trial run for a crisis management program is on a case-by-case basis for each company and based on their specific risk appetite; however, examples could include incoming reports of misplaced data deemed not highly sensitive (such as escalated from a manager or potentially from the hotline system), strong but not destructive weather in certain regions where your company operates (such as a strong noreaster, as example), and so on. By getting the organization in the habit of engaging a plan even for more mundane issues, a CMT can be ready to run the plan, on a more scaled-up form, for even the most serious crises.

> "the only way to know if the plan would work in an actual event is to put it into practice, whether in a real situation or in a well-designed simulation. Periodic table-top exercises and other response drills take time and should be executed thoughtfully. But if done right, they can make a marked contribution to an organization's overall level of preparedness and ensure that their plan will be relevant and useful in the event of an actual crisis."

CONDUCTING DRILLS ON KEY RISKS

The following are steps recommended for any organization interested in developing a strong crisis planning process and table top exercise:

- Try to have everyone in the room.
- Remember who is involved will depend on the scenario.
- Make sure the scenario is well-designed, emphasizes different components of the response, requires to make judgments in real time.
- Remind people not to fight the scenario. They should assume it's well designed.
- Reinforce people should be realistic and do not assume you will all overperform.
- Practice escalating triggers to give a realistic sense of what it would look like if it really happened.
- Don't set thresholds so high people won't use the plan (i.e., can put in media monitoring at an early stage).
- Watch the size of the group, as you want people to be engaged and participatory.



SECTION THREE:

OUTSIDE COUNSEL: AN UNDERUTILIZED ASSET

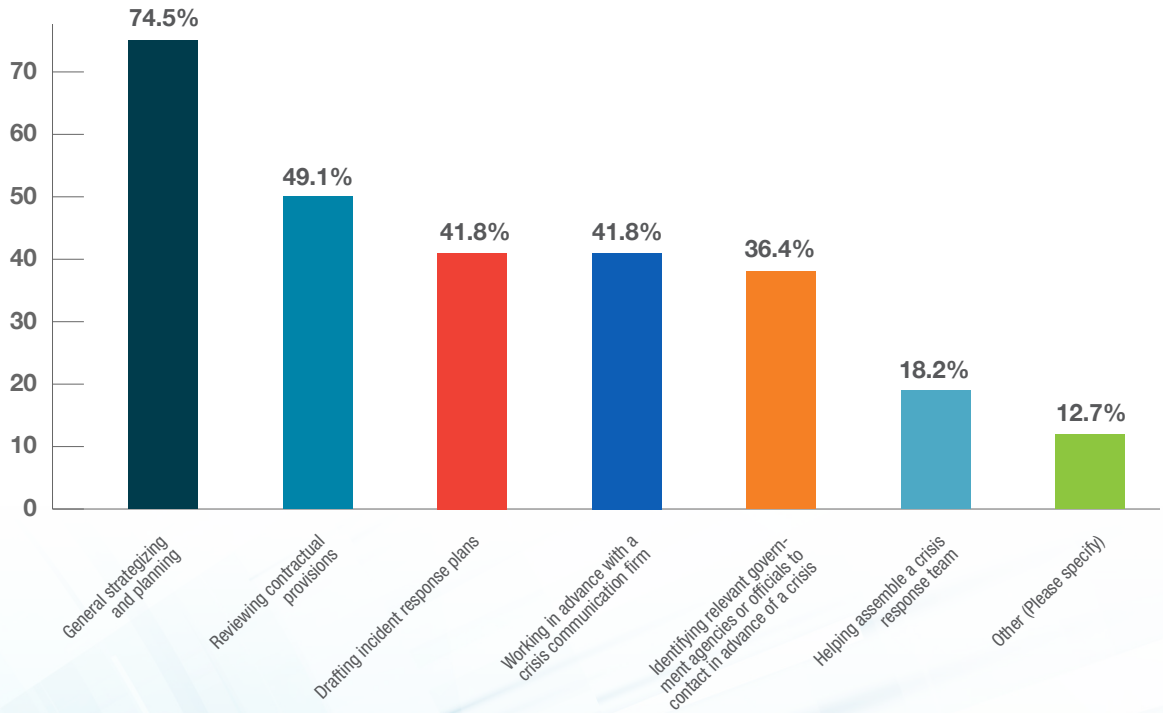
Although crisis management might seem like an inherently in-house role, that is often not the case. Some organizations, especially smaller ones with less legal capacity, might benefit from bringing in outside advisors.

The role and the support of outside counsel can be wide ranging. Three-quarters of companies who employ outside counsel on their CMTs do so for general strategizing and planning, but the benefits of doing so go beyond strategy and planning. For example, nearly half of the organizations that use outside counsel for CMTs do so for reviewing contractual provisions (49.1%). Approximately two out of five use outside counsel for advanced planning with communications firms (41%), which is a critically important element of a crisis response plan. There can often be tension between the legal team and the communications team, as generally the communications team is trained to get a message out to stakeholders as quickly and efficiently as possible, while a legal team is often trained to keep information contained in order to avoid exposure to additional liability. This trend is changing as the best crisis management teams understand both needs and work hand in hand to ensure the company is protected while simultaneously getting clear and open out to its stakeholders.

"Law firms have historically been wary of the PR and communications perspective," says Smithline. "But it's increasingly seen as a powerful tool in investigations as the media can often drive the narrative. There's a trend where during a crisis event companies used to keep allegations confidential but today there is a greater chance you will be battling both PR and legal challenges and so companies need to be prepared to have a media strategy with a mix of in-house and outside support."

Cohen agrees, saying, "it used to be that saying 'no comment' was the default. Companies are rethinking that and considering ways to be more affirmative if they can. These communications plans need to involve the lawyers and outside counsel are having a lot more involvement than they used to have. Reputational harm is such a series thing, but you need to craft your messaging in a way that doesn't also hurt the credibility of the investigation."

HOW DOES YOUR ORGANIZATION WORK WITH OUTSIDE COUNSEL IN CRISIS RESPONSE PLANNING?



Beyond the PR and communications element, outside counsel are also hired by companies for drafting incident response plans (41.8%). Nearly a third of the companies report using outside counsel to help identify key enforcement agencies or officials to contact in advance of a crisis (36%). And interestingly, outside counsel are even being used to help to assemble a crisis response team (18.2%), reflecting the important perspective outside counsel can bring to a CMT based on their broader client experience.

Outside counsel can also be an excellent resource in helping companies enhance the areas of their crisis management plans where they feel the least prepared. Interestingly, though terrorism and cyber breach were the top two responses for which respondents felt least prepared – as mentioned earlier in this report – only 34% of those who cited terrorism had a crisis management plan in place and worked with outside counsel in advance of a crisis, while only 28% of those most fearful of a cyber breach had taken these two basic steps toward preparedness.

Depending on the size of your overall organization, the maturity of your crisis management plan, and the legal resources at your disposal, bringing in outside counsel may be an excellent way for your organization to improve its crisis management capacity. Outside counsel who specialize in crisis response will have experience dealing with situations that your in-house team may not anticipate, and they may have templates or other resources from which a nascent program can build.

In addition, outside counsel that have extensive experience in investigations will understand how to address privilege, which warnings must be given before conducting interviews if the company is interested in using that information with regulators, and much more. Consider preserving privilege as well; it may be wise to retain other experts through your outside counsel to preserve privilege. Finally, if you are addressing regulators as part of the crisis, having independent outside counsel will be a must.

Having outside counsel tapped as resources for your CMT, even if they aren't involved in every stage, is also a way to ensure that you have subject matter expertise available for certain kinds of specific crises, such as terrorism, workplace violence, or environmental disasters, in which your team may not have experience. If your operations are multinational, it will likely also pay to retain a firm with crisis management capacity in all countries where you have major operations who know the relevant legal landscape and would be prepared to engage with local authorities in a crisis situation.

In all cases, rapid response is essential, and an organization can find itself navigating complex waters if leadership does not consider a strategy until faced with a crisis. Experienced counsel can bring an additional outside perspective to the table both in the preparedness phase and in the actual event.

Conclusion:

It likely comes as no surprise that cyber readiness remains a pressing focus area for companies' crisis management teams and that companies are increasingly focused on how to respond to allegations relating to workplace harassment. Our survey underscored the importance of those areas while also highlighting the extent to which sophisticated organizations also plan for ever-present risk areas, including corruption and bribery, IP theft, terrorism, product recalls, and the other areas explored in this report. Among the recurring themes of those interviewed is that crisis management teams must remain vigilant and practice on-going training and preparation for a possible future event. As explored in this report, the best and most prepared companies:

- have a crisis management team comprised of cross functional leaders, all of whom must have good working relationships and regular communication;
- conduct drills and benchmark their crisis management programs on a regular basis;
- have ongoing training and communication programs in place throughout the year; and
- increasingly are engaging outside counsel to help coordinate crisis planning and to be available in the event of an incident.

While it will never be possible to prevent a serious event from occurring, proper planning and training will ensure your company is prepared to handle an unexpected crisis should one arise down the line.

REPORT CONTRIBUTORS

Erin Bosman
Chair, Product Liability and Counseling

David Newman
Of Counsel, Global Risk & Crisis Management and National Security

Ruti Smithline
Co-Head, Investigations & White Collar Defense

John Carlin
Chair, Global Risk & Crisis Management
Co-Head, National Security

Lisa Phelan
Partner, Global Antitrust Law and Investigations & White Collar Defense

Eric Akira Tate
Co-Chair, Global Employment and Labor

Carrie Cohen
Partner, Investigations & White Collar Defense
Co-Chair, Workplace Misconduct Taskforce

John Smith
Co-Head, National Security
Partner, Global Risk & Crisis Management and Investigations & White Collar Defense

Christine Wong
Partner, Investigations & White Collar Defense

METHODOLOGY

Morrison Foerster and Ethisphere partnered to create the Crisis Management Benchmarking Report conducting an online survey of senior-level executives working in ethics, compliance, risk management, and other fields related to crisis management. Survey responses were collected in the spring of 2018.

The survey produced 248 complete and partial responses. Respondents were not required to answer every question.

Responses were split roughly evenly between private (4%) and public (38%) companies; an additional 12% represented non-profit organizations, 4% represented government entities, and 5% represented academic institutions.

Nearly half (46%) of organizations were headquartered in the United States, followed by Western Europe (19%), Canada (12%, and Australia/New Zealand/Oceania (9%).

The median worldwide revenue for respondent organizations was $1 billion to $5 billion (USD).

This was a self-reported survey from Morrison Foerster and Ethisphere's audience of ethics and compliance professionals, and Ethisphere did not attempt to verify or audit the data reported by survey-takers.

MORRISON
FOERSTER

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

www.MoFo.com/CrisisManagementSurvey