BIHC NETWORK

ELEVATING BLACK EXCELLENCE
VIRTUAL REGIONAL SUMMIT SERIES

A Showcase for Black Partners

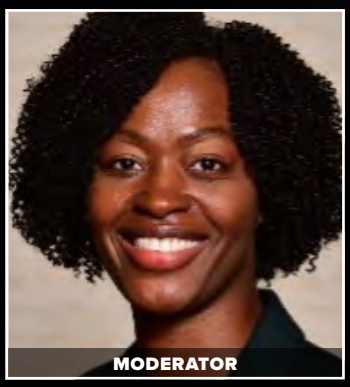
Session 703

CRISIS MANAGEMENT: WHAT TO DO WHEN DISASTER STRIKES

Amber Finch
Reed Smith LLP

Arian June
Debevoise & Plimpton LLP

Camille Varlack
Bradford Edwards & Varlack LLP



Shyka Scotland
PwC

EXECUTIVE SUMMARY

Crisis Management: What To Do When Disaster Strikes

MODERATOR:

Shyka Scotland, *Director,* **PwC**

PANELISTS:

- **Amber Finch,** *Partner,* **Reed Smith LLP**
- **Arian June,** *Partner,* **Debevoise & Plimpton LLP**
- **Camille Varlack,** *Partner,* **Bradford Edwards & Varlack LLP**

OVERVIEW

This panel of crisis management experts shared advice to plan for and effectively manage a crisis in the current environment. Best practices include planning in advance to avoid panicked decision making, having policies in place, and ensuring the right team of experts is engaged, which can include expert outside counsel. Also, anticipating and planning ahead for specific scenarios such as a data breach, a whistleblower, or an allegation of sexual harassment is helpful.

KEY TAKEAWAYS

Even if more crises are not occurring, the appearance and cost of crises have accelerated.

Every day it seems there is another crisis event, of all shapes and sizes. Whether this is due to more crises happening, more being reported, or more attention paid to those that are reported, crisis management is a constant drumbeat. Among the trends affecting crises are:

- **Changed environment.** Even if there is not more misconduct, the environment reflects different expectations around corporate conduct, especially by executives. Both the *Me Too* and *Black Lives Matter* movements changed expectations for acceptable behavior.

BIG IDEAS

- **Crises occur constantly, making it necessary that businesses plan ahead to manage them.**
- **While every crisis is different, the keys to managing them are people and policy.**
- **Scenarios show how best to manage through common crises involving a data breach, a whistleblower leak, and an allegation of sexual harassment.**
- **Any crisis management plan must include insurance.**

- **Virtual life.** Working from home changed how people interact. Being more "comfortable" seems to have led to plenty of instances of inappropriate workplace actions and bullying. People are comporting themselves differently. In addition, working virtually has been accompanied by increased cybersecurity incidents.
- **Generational change.** Younger professionals are not tolerating behavior that older employees put up with. "Enough is enough," younger people are saying.

While experiencing crises is not new, crises are being magnified and the cost of managing crises has increased. In referring to data breaches, instances of sexual harassment, and more, Ms. Finch said, "The dollar amounts associated with these issues have significantly increased," as have the costs of defending cases. Runaway jury verdicts have also gone up. From an asset protection standpoint, companies need to make sure they have adequate insurance policies in place and that those policies are renewed and regularly reviewed.

In planning for and managing any crisis, policy and people are critical.

The key building blocks of crisis preparedness are having policies in place and gathering the right people.

Policies and procedures

It is essential to have an incident response plan in place prior to any event to prevent poor decision making. Know the immediate steps because the first hours are critical. It is also important for all employees to know the incident notification procedures; for new employees this can be part of the onboarding process.

"Having that plan will provide the framework for actions where key decisions are made ahead of time, instead of having to make those decisions under pressure."

— Amber Finch, Reed Smith LLP

The policy and plan should focus on first understanding the facts and ensuring that any public statements are drafted carefully so they do not get in front of the facts. Also important early on is to assess whether the crisis implicates internal policy, regulatory, or statutory rules.

People—who are your team

Managing any crisis requires a team. The exact composition of the team may vary based on the crisis, but common participants include:

- The CEO as the public face of the company and the executive management team
- The CFO or a representative from finance
- A senior HR person to communicate with employees
- An IT leader
- The GC or a representative from the legal team, as well as outside counsel
- Customer relations to coordinate customer communication
- Other team members may include PR and crisis communication; for a data breach it may be necessary to have forensics and data restoration experts

Being surrounded by the right people means the core team members, internal and external, all have a purpose. Avoid making the group too large. They should be experts in their field, and company leaders need to trust their expertise.

"It should really be just those trusted advisors who have a need to know. And the reason for that is you have to assume that more information about the crisis could leak at any moment."

— Arian June, Debevoise & Plimpton LLP

Depending on the nature of the crisis, there are specific concerns to keep in mind and actions to take.

In addition to the general playbook of preparing by having policies in place, gathering the right people, and investigating all facts, certain incidents raise particular considerations. Scenarios discussed were:

A data breach or cyberattack

Because a cyber event attacks the organization's computer network, it is vital to have an alternate plan, such as texting, to communicate with employees. It is important to be able to communicate within the first hours of an event. Other tips include:

- IT's immediate role is to identify how and when the breach occurred, the seriousness of the incident, and how to contain it, and to ultimately resolve the incident.
- Organizations must be extremely careful with public statements about a breach since any statement may trigger notification requirements in certain jurisdictions.

A "whistleblower" leak

When a company faces an external whistleblower leak, such as to the media, it means somethings within the company has already gone wrong. Studies consistently show that most employees first attempt to use internal reporting mechanisms and only turn to external sources when internal sources are ineffective.

When faced with a public crisis initiated by a whistleblower, the first step is to dig into the facts. Working closely with communications ensures that public statements or denials do not get ahead of the facts. The nature of the specific allegations drives the facts and next steps, since the incident could be related to financial misstatements, serious product failure, or allegations against the CEO. Basic questions are:

- Is there merit to the allegations?
- How long has anyone known?
- How high did it go?
- Has it already been corrected?

A key question will be determining whom to speak to in gathering facts. This leads to the sensitive question of searching for the source of the leak. Many allegations carry potential criminal exposure, leading the government to closely scrutinize a company's actions, even though a press leak is not legally protected whistleblower activity.

Media stories are frequently followed by subpoenas. So even though a company is concerned about theft of sensitive information, the government will view it differently. Moreover, it is vital that the search for the source of a leak not distract from the need to understand the facts around the allegations themselves.

Even when a specific employee is suspected of being the whistleblower, companies need to tread carefully and consider the risks before acting against the individual. Of course, an official report to the government, rather than the press, is protected whistleblower activity.

"It comes down to a balancing exercise. We want to safeguard any confidential data. But on the other hand we also want to avoid any further regulatory scrutiny and certainly avoid any criminal exposure."

— Arian June, Debevoise & Plimpton LLP

"Me Too" scenario

Surprisingly, companies still respond improperly to sexual harassment allegations. Employers need to have policies in place and training. Companies must take every complaint seriously and conduct a prompt, professional investigation. Appropriate policies and procedures enable employees to understand where to make allegations and what to expect from an investigation. It is important to have a roadmap for what to do and how to look into the issues. Documentation of all steps is vital.

"It's not your perspective on whether or not the conduct that is being described constitutes harassment. You have to think of it from the perspective of the individual."

— Camille Varlack, Bradford Edwards & Varlack LLP

Organizations need to make clear their policy of anti-retaliation and communicate this policy. Sometimes it is necessary to clarify whether alleged behavior violates the law or company policy, or simply shows poor judgment. Threats of publicity or litigation can elevate an incident.

Specific sensitivities around alleged CEO misconduct

If the CEO is accused, following the established procedures is critical. Clear demarcation of responsibility for conducting the investigation is necessary. Briefing the board early can help alleviate potential pressures, and often it helps if the board removes the investigation entirely from the CEO's chain of command and brings in outside counsel to conduct the investigation, reporting to the board.

"It's important that you adhere to what the protocol is, notwithstanding the seniority of the individual you are investigating."

— Camille Varlack, Bradford Edwards & Varlack LLP

It may be useful to retain specialized external PR resources to help the company and the management team deal with the allegations, especially when an accuser takes a highly visible stance. Even so, the company may not yet know the facts around the allegations, the investigation may be ongoing, and the company's public statements may need to stay at a high level.

Settlements and NDAs may be a less viable option to keep these matters private than in the past, as states now question the enforceability of this type of NDA.

Insurance plays a valuable role in crisis response; it is important to act within the coverage window.

Crisis management insurance is a key part of any crisis readiness plan. Many executives are not aware of the array of things that can be covered. Direct financial assistance for expenses incurred or losses from perils, along with outside counsel, PR consultants, and data forensics, are all possibilities. A data breach may involve cyber coverage but can also involve professional liability lines, property lines, or other types of coverage. Thus, it is critical to quickly notify the carrier when an event occurs. Timely notification can make a significant difference in ensuring that the company realizes all potential policy benefits.

"From an asset protection standpoint, make sure that your insurance policies are in place, that they are renewed and looked at on a regular basis."

— Amber Finch, Reed Smith LLP

BIOGRAPHIES

MODERATOR

Shyka Scotland

Director, PwC

Shyka Scotland is a director with PwC's Discovery Managed Services practice, where she focuses on using design thinking to solve process complexity within legal departments. She has more than 13 years of experience providing strategic solutions in domains such as eDiscovery, investigations, legal technology, and information governance. She specializes in carrying out all aspects of a project from conception to execution and feedback. She has experience building and managing eDiscovery teams as well as developing and implementing strategies designed to meet clients' corporate discovery needs. She is experienced in deploying technology and advanced methodologies to improve the value proposition for services attendant to risk, compliance, and the legal sphere. Prior to joining PwC, Shyka has led discovery activities on some of the largest and most complex litigation and global regulatory investigation matters across financial services, life sciences, energy, and consumer sectors. She advised on a number of Discovery advisory projects, which involved (re)designing solutions to improve client eDiscovery programs, workflows and procedures, and leading practice implementation for several FTSE 250/Fortune 500 companies. Shyka holds a J.D/MBA from American University Washington College of Law and Kogod School of Business. She maintains a law license in the state of New York.

Amber Finch

Partner, **Reed Smith LLP**

Amber Finch is a member of Reed Smith's Insurance Recovery Group and is managing partner of the firm's Los Angeles office. Amber is a go-to lawyer for creating effective risk management solutions. With her litigation background, she has helped her policyholder clients recover hundreds of millions of dollars in insurance proceeds. Amber represents a litany of clients from start-up businesses to middle market and Fortune 500. She helps companies manage risk by negotiating broader insurance coverage on the front end, negotiating insurance and indemnity provisions in deal contracts, assisting with tender and collection on insurance and indemnity claims, and litigating insurance and indemnity disputes. Most recently, Amber represents companies with business income interruption and property damage losses arising from the COVID-19 pandemic, and advising clients impacted by the Russia-Ukraine war. Amber is a past president of the Black Women Lawyers Association of Los Angeles, and a board member of Legal Aid Foundation of Los Angeles. Amber's recent honors include being listed in *Savoy* as a "Most Influential Black Lawyers"; Corporate Counsel's Women, Influence and Power in Law Awards for DE&I Law Firm Champion; Empower's Ethnic Minority Role Model List; *Los Angeles Business Journal's* Leader of Influence: Top Litigators & Trial Lawyers; and *National Law Journal's* Crisis Leadership Trailblazer.

Amber Finch
Reed Smith LLP
afinch@reedsmith.com

Arian June

Partner, **Debevoise & Plimpton LLP**

Arian M. June is a Debevoise & Plimpton LLP litigation partner and a member of the firm's White Collar & Regulatory Defense Group. Recognized by *The Network Journal* as one of 25 Influential Black Women in Business (2020) and named to the *Benchmark Litigation* 40 and Under Hotlist (2021), Arian's practice focuses on crisis management, government and internal investigations, sensitive investigations, securities enforcement defense, whistleblower response, and white collar criminal defense. She frequently advises boards of corporations, educational institutions, and other organizations in sensitive investigations, including board-directed independent inquiries of allegations involving sexual misconduct, racial intolerance and related matters. Arian also represents financial institutions, publicly traded companies, investment advisers and senior executives in complex regulatory matters before the SEC, DOJ, FINRA and numerous state attorneys general and state securities regulators. Arian's work includes matters involving allegations of securities fraud, insider trading, accounting and corporate disclosure issues, violations of the Bank Secrecy Act, cyber-intrusions and sales practices violations, including matters involving foreign exchange products and the distribution of life insurance products. She lectures and publishes frequently on government investigations, SEC enforcement issues, and corporate whistleblowers.

Arian June
Debevoise & Plimpton LLP
ajune@debevoise.com

Camille Varlack

Partner, Bradford Edwards & Varlack LLP

Camille Joseph Varlack is a founding partner and the chief operating officer of Bradford Edwards & Varlack. With over 16 years in public and private sector legal and operational leadership, she brings a calm and disciplined approach to risk management and is an expert at solving complex organizational problems. Ms. Varlack has expertise in managing risk in large organizations and is known for her ability to successfully navigate large-scale crises. In summer 2020 she served as a member of the New York State COVID-19 Task Force. Ms. Varlack served in the New York State Executive Chamber as deputy director of state operations, chief risk officer, and special counsel, in charge of leading teams through statewide crises as well as responding to a multitude of public health crises. She worked with local and federal law enforcement officials and conducted internal investigations on a range of subjects including governance, financial compliance, and employment/HR matters. As chief risk officer she was responsible for managing audit, compliance, and internal control issues for state agencies and was instrumental in the development and implementation of the first statewide enterprise risk management system. Ms. Varlack advises businesses on risk, legal crisis management, employment litigation, and the resolution of related complex business matters.

Camille Varlack
Bradford Edwards & Varlack LLP
cvarlack@bradfordedwards.com