

Reproduced with permission from Corporate Accountability Report, 189 CARE, 10/02/2017. Copyright © 2017 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

**RISK MANAGEMENT**

**Managing Corporate Risk in Uncertain Times**



BY TROY MORGAN AND PRESTON PUGH

*Troy Morgan is a compliance officer and legal counsel with over 15 years of government, corporate and operating unit experience, managing legal and compliance functions in global organizations in the medical device and pharmaceutical industry. He is currently Vice President and Chief Compliance Officer at Bioverativ, a rare disease biotech company located at Waltham, Mass., where he is responsible for leading global efforts to facilitate compliance with emerging and complex health-care laws and regulations.*

*Preston Pugh is an investigations and litigation member of the law firm Miller & Chevalier in Washington, D.C. He has extensive experience as outside, corporate, and government counsel representing large organizations in complex civil and criminal litigation, internal investigations, and government investigations. He is a twice-appointed compliance monitor, having served in those roles for several years, and a former Assistant U.S. Attorney. He has served as Senior Counsel for Investigations and Litigation at GE Healthcare, and as seconded investigations counsel at Boeing's Integrated Defense Systems.*

“Those who cannot learn from history are doomed to repeat it.” – George Santayana.

With the advances in technology, shifting geopolitical landscape and ever-increasing enforcement by federal and state regulators, today’s executives may justifiably feel that the ground beneath them is ever unsteady. What’s worse, the timing of improbable, highly disruptive crises is almost impossible to predict, and they may seem more likely than ever to occur. These corporate crises over recent years have been triggered by predictors that we have seen before: overly aggressive growth strategies without proper controls; decentralized reporting structures that allow divisions to run themselves with little to no oversight from corporate headquarters; tolerance of short cuts; and “star gazing” or allowing senior executives to act with impunity.

With that said, rather than focusing on predicting those events, executives should instead ensure their companies have the right processes in place to manage them. The question is when, not if, these crises will occur.

In this article, two colleagues and former coworkers, Troy Morgan, Chief Compliance Officer at Bioverativ, and Preston Pugh, Member at Washington, D.C., law firm Miller & Chevalier, share their views on a few ways executives can reduce their vulnerability in these uncertain times.

**If it was ever acceptable to have a good compliance program on paper, but not in practice, that sure isn’t the case now**

Corporate scandals continue to grab headlines across industries. State Street, where it was alleged that the firm settled charges that it fraudulently charged secret markups to customers, Insys Therapeutics, where top executives were indicted for paying kickbacks to physicians, and the recent Equifax data breach, where executives are accused of trading large amounts of stock before the breach was announced and the stock tumbled, are all good examples of ethical conflicts that companies are facing today.

While these unethical business practices are not new or novel, public perception and public exposure to them

are changing. Transparency is not only a government requirement, it is now viewed as a public right. Everyone has access to information and everyone is watching. Many of these cases have been brought to light by internal whistleblowers motivated by frustration, believing that their companies did little to resolve the problems they raised, or for financial reasons, eager for a share of the recovery from actions pursued and settled by agencies such as the Securities and Exchange Commission and Department of Justice. While in the past, some corporate misconduct did not see the light of day, today, with internal and external watchdogs and open access to data, the chances of exposure are high if not expected.

### **Understand what an effective compliance program looks like**

Federal and state regulators continue to show what we have known for some time: companies need a personal, proactive and progressive approach to risk management. In fact, if they do start to ask questions about the integrity of a company's business practices, appropriate risk management and compliance programs are often the first places they will look.

Establishing the right risk and compliance approach starts with ingraining a culture of integrity with the oft-used **tone from the top** of the organization. Employees need to witness executives making compliance a priority and exhibiting compliance and integrity in an open and public manner. Next, executives need to proactively listen to their employees (such as with a bona fide "open door" policy), take concerns that are being raised seriously and address them efficiently. Finally, because many of the conventional internal controls used to detect and manage compliance issues are no longer effective, companies should empower trained and dedicated compliance officers who understand how to implement effective compliance programs.

---

### **Merely having a code of conduct and internal "paper program" policies is not sufficient.**

---

Merely having a code of conduct and internal "paper program" policies is not sufficient. These cannot withstand the scrutiny of the government, potential internal whistleblowers, or the public eye. Companies need unique, innovative and business-integrated compliance procedures and effective training programs that ensure every employee understands and implements the company's compliance principles. Companies must also frequently monitor their activities and spend, look for the early warning signs, and then immediately respond and document the results of any investigation or inquiry. Auditing retrospectively after a crisis has occurred is not enough. You need a program that proactively engages employees and interactively monitors your activities to truly understand where the company needs to improve. Earlier this year, the DOJ Fraud Section released a key guidance document entitled, *Evaluation of Corporate Compliance Programs* ("Evaluation Guidance"), <https://www.justice.gov/criminal-fraud/page/file/937501/download>, that is a very helpful reference

for what the government's expectations are for an effective compliance program, at least at this time.

Creating a culture dedicated to corporate integrity needs to be a part of a company's DNA. It is a foundational investment that is critical in building and maintaining a company's most important assets: trust and reputation. If the leadership of an organization truly values and rewards employees for *doing things right*, the business will respond by *doing the right things*.

### **If an employee raises a concern, use the "headline test." Think about how your company's response would look on the front page of the news**

During our time working together, we have responded to many concerns raised by employees. While some may have been minor issues or misunderstandings, others highlighted real issues and provided genuine opportunities for companies to learn and improve. The important thing is to take every concern seriously. Companies need only mishandle one significant complaint to cause a problem, especially when it later becomes public and exposes a sensitive issue. Unfortunately, hindsight truly is 20/20.

In considering this issue, we have learned that these situations are best mitigated by having an effective escalation and investigation process. If an issue is escalated, a company needs to react quickly and have an established plan in place to determine who will conduct the investigation and how the investigation will proceed. There are many situations when a matter can be handled internally. However, there needs to be clear objectivity in the process, and an investigation team needs to be properly trained. Accusations involving violations of a company's code of conduct should not be taken lightly, as the initial concern raised could be just the tip of the iceberg.

There are also situations when you should bring in outside counsel to conduct the investigation, specifically if the matter has a potential to lead to litigation or disclosure to a government agency. An investigation that is not well thought-out at its inception can easily run into issues. The need to have a formal process in place and carefully plan an investigation and show objectivity and independence cannot be overstated.

Companies need to have the resources and processes in place in case a serious issue is raised. Delay or inefficiency in handling a report only amplifies the risk and may expose the fact that a company may not be taking employee concerns and internal compliance seriously.

### **To stop corporate misconduct, companies first need to understand that its origins are not always readily apparent**

Too often when we read stories about an employee who has been prosecuted for white-collar crime, we typecast the offender as a "villain," someone who is "not like us." In reality, studies of white-collar crime show that, many times, the offenders are not so different from the rest of us. It is not unusual for the target of a significant investigation to be polite, charming, and hardworking.

Why does fraud happen? As explained by criminologist Donald Cressey, the answer lies in "Pressure, Opportunity and Rationalization," also known as the

“Fraud Triangle.” Pressure to commit fraud can come from difficult-to-reach sales and performance goals, family need, illness or just the desire to improve one’s financial standing. Uncontrolled access to company assets such as cash and corporate credit cards, and control over expense accounts, can provide the opportunity. Rationalization describes how an actual or potential offender justifies his actions to himself because perhaps he feels underpaid and overworked, or feels that the fraud has no victim, or even that his actions are temporary and will be overlooked. When pressure, opportunity and rationalization combine, it can motivate the employee to fudge a time sheet, take a few extra dollars, or even give a slightly altered report. Over time, the employee’s actions worsen, and by the time they are discovered, what the employee once thought would be a “white lie” has now grown into a much larger problem that they’ve lost control over.

To effectively manage fraud risk, executives must identify the gaps in their companies’ controls and business processes. Is employee compensation consistent

with others in the market? Are the incentives that the company provides for meeting performance goals excessive, or reasonable? Frequent and comprehensive internal audits and risk-based monitoring are important, but they are also not the entire solution. The right controls need to be in place based on the company’s risk profile. Simply because an employee is trusted, familiar or friendly does not mean that we should look away when we see evidence of cutting corners.

## Conclusion

The investment needed to create an ethical culture and effectively manage compliance risks are a cost of doing business the right way. However, the true costs of leaving those risks unaddressed—including harm to the company’s brand, loss of investor and market trust, and organizational and personal liability—are much greater. Thoughtful action needs to be taken at the most senior levels to ensure compliance and an ethical culture, and often that does not come easily.