

Reproduced with permission from Corporate Accountability Report, 56 CARE 56, 10/28/15. Copyright © 2015 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

INTERNAL INVESTIGATIONS**Sidley Austin's David Hoffman Discusses Key Considerations
For Companies Undertaking Internal Probes During Emerging Scandals**

Earlier this year, an internal investigation led by Sidley Austin LLP partner David Hoffman blew the lid off the American Psychological Association's (APA) role in the Bush administration's "enhanced interrogation" program. The APA board hired Hoffman to conduct an internal investigation after an explosive book by New

York Times journalist James Risen in October 2014 suggested that the APA colluded with the CIA and the Defense Department to assist the interrogation program. After interviewing 150 witnesses around the country and reviewing tens of thousands of documents, the Sidley team issued a report in July this year. The team found that leading APA officials did in fact collude with Defense Department officials to create and maintain permissive APA ethics policies that allowed psychologists to participate in potentially abusive detainee interrogations at Guantanamo Bay and elsewhere.

In an interview with Bloomberg BNA's Yin Wilczek, Hoffman says the APA case offers key lessons for companies caught in emerging scandals. He also says that the Justice Department's new policy on individual culpability may complicate matters,¹ and that data breaches are a growing area for internal investigations.

BLOOMBERG BNA: In light of the APA situation, what do you see as some of the key challenges confronting companies that want to embark on an internal investigation?

Hoffman: Two of the most important considerations for companies that are deciding whether to initiate an internal investigation are: what is the likely scope of the investigation, and what does the company hope to ac-

David Hoffman is a partner at Sidley Austin in its Chicago office, where he is co-head of the White Collar Practice in Chicago and leads that office's work on data-breach-related litigation and investigations. Among other career highlights, Hoffman was an Assistant U.S. Attorney in Chicago from 1998 to 2005, and Inspector General of the City of Chicago from 2005 to 2009. As Chicago IG, he led a 65-person office that conducted corruption investigations, and he established and supervised an external audit team that examined internal controls and compliance procedures throughout a \$7-billion-per-year, 36,000-employee entity.

He is also a Lecturer in Law at the University of Chicago Law School where he has taught "Public Corruption and the Law" for the past six years. He is a graduate of Yale and the University of Chicago Law School and clerked for Chief Justice William Rehnquist.

¹ See the Yates Memorandum, available at <http://www.justice.gov/dag/file/769036/download> (13 CARE 1952, 9/11/15).

comply by conducting the investigation. Both of those questions can be very difficult to answer at the beginning, especially the second question regarding the company's goals.

The APA case was a fairly unique situation. How those key considerations played out with the APA was really quite interesting.

One of the biggest issues for the APA over the last 10 years has been the fallout from its decision during the Bush administration to issue ethical guidelines that allowed psychologists to participate in national security interrogations. There was intense external and internal criticism that these guidelines effectively permitted psychologists to participate in abusive interrogations and, in some circumstances, torture. Those who had set up the ethics guidelines strongly disputed this claim. But a substantial percentage of psychologists were deeply and passionately concerned about the issue, and saw it as a critical ethical problem that affected the very integrity of the profession.

The day after Risen's book was published, the APA issued a lengthy statement disputing all the claims made by Risen and the APA critics. But a couple of weeks later, the APA board adopted a different approach, and decided that the association needed a thorough, credible and independent investigation to figure out what happened, and a public airing of the investigation's findings regardless of what they were. And so they hired us to conduct an independent investigation, and they announced it publicly. They also announced that they would make our report public, without modifications. Their announcement stressed that they had instructed us to make our own independent judgments about how to conduct the investigation and what conclusions to draw, and said that we were to follow the evidence wherever it led, whether it made the APA look good or bad.

In the realm of internal investigations, it's atypical for a client to make an extensive public statement at the beginning of the engagement emphasizing that the investigation will be independent, at least when the government has not required an independent monitor, for instance. But there are times when it is critical for an entity's integrity or reputation that it establish publicly that the investigation will be truly independent and that there shouldn't be any doubts about the credibility of the investigation. Another example is Penn State University's investigation of the Jerry Sandusky scandal.

It also is unusual for there to be a public commitment at the beginning of the engagement that the report from the internal investigation will be made public. Internal investigation reports are sometimes made public, but the APA went out of its way to announce from the beginning that it would make the entire report public, obviously before knowing what the report would say or where the investigation would go.

The attorney-client privilege is “one of the trickiest areas of the law.”

This connects back to what I was saying about having an understanding at the beginning of the matter about what your goals are in having an investigation

conducted. Clearly, the APA's goal was, “We need to show our critics and our membership that we are going to have someone produce a credible, thorough description of what happened. In order to do that, we have to hire someone who can be independent and can have the credibility to show that we've gotten to the bottom of the facts.” Over the years, an intense level of cynicism had grown around this issue, not only about the APA's initial decisions during the Bush administration but also as to the manner in which the APA had responded to its critics in the years since. Everyone knew that how they set up the internal investigation, what instructions they gave us, and how we conducted the investigation would be the subject of intense scrutiny in both the psychology and intelligence communities.

The APA would have anticipated of course that if the report was critical, there would be further negative attention in the short term. But it appears to have weighed the pros and cons and said, “We would rather have a factual public airing of what happened even if that comes with some criticism, rather than the alternative, which is to do what we've been doing.” Their board was clearly thinking that for the long-term health of the APA, it needed to get beyond this issue, and they couldn't do so until they provided a credible, independent accounting of what happened.

That lesson translates to companies in many situations where they face the decision of, do we conduct an internal investigation, and if so, what should the scope be.

BBNA: Are there other considerations?

Hoffman: In addition to the scope and goals of the internal investigation, a third challenge for companies is handling potential disclosures to the government and/or interactions with the government.

The new guidelines recently announced by the DOJ signaling the department's increased focus on individual culpability certainly increase the difficulty in an already difficult area for companies. It's a minefield whenever potential wrongdoing is brought to a company's attention. There are a lot of judgment calls to be made.

While the DOJ's new policy may not make internal investigations more difficult, it will increase the complexity of a company's decision-making about whether or how to disclose information to the government and how to interact with the government.

The fourth challenge for companies is the attorney-client privilege. This is one of the trickiest areas of the law. Perhaps the biggest pressure point in this area is when a company is considering whether to disclose the results of its investigation to the government, because there are always potential consequences with respect to privilege. It's not black and white in terms of whether all, some, or none of the protections from the attorney-client or work product privileges remain in place. It can be very context specific.

To preserve the privilege when there is disclosure requires careful management of both the privilege during the investigation and then discussion of how the privilege will be affected if there is disclosure.

The recent decision in which the D.C. Circuit allowed KBR to shield certain internal investigation documents from a whistle-blower who had sued KBR under the

False Claims Act² was helpful because it confirms that if you follow *Upjohn*, then your investigation is a presumptively privileged process. Outside counsel needs to work with the client to be diligent about protecting that privilege, but it certainly can be done.

BBNA: What are some of the major pitfalls that companies should be aware of in initiating an internal investigation?

Hoffman: Number one, it can expose problems within the company. Second, it can be disruptive, and third, it can be costly.

These are discussions that we have in a very explicit way with boards and chief executive officers and general counsel before embarking on an internal investigation because these are legitimate concerns. However, it is always critical to consider the alternative.

Companies that already are facing a potential scandal can't compare the prospect of conducting an internal investigation with an ideal world. It obviously has to be compared with, "What would the world look like if we don't do an internal investigation?" That's not to say that an internal investigation is always the right answer, but the decision not to conduct a credible internal investigation will often create at least three problems: 1) you're potentially leaving an important corporate problem unaddressed; 2) you may create the likelihood that a whistle-blower will turn to the government or the press instead of the company's internal resources to deal with the problem, which is a very important point.

And 3) the decision not to deal with a problem that's presented to the company may be used against the company by the government or in litigation as evidence of the company intentionally ignoring the problem.

Again, every situation is different, so it doesn't mean that this analysis automatically points toward doing an internal investigation. But reviewing the costs and benefits of conducting an investigation versus not doing one is important in every situation. If a significant problem has been brought to the company's attention, there are going to be very substantial downsides in not doing an investigation. And that needs to be weighed against the alternative of doing one.

BBNA: What are some new developments in the world of internal investigations?

Hoffman: The SEC's case against KBR for impeding federal whistle-blower protections is one recent development.

One of the things to keep in mind is that the SEC will look askance on situations in which an employee is prohibited from telling the SEC about problems at the company, or if the company makes that very difficult to do. The key word in the regulation is "impede." You can't impede someone from communicating directly with the SEC about a possible securities law violation. Importantly, this doesn't mean that a company is prohibited from keeping its internal investigation confidential or from telling employees it is confidential, because there is a distinction between the process of conducting an internal investigation and the underlying facts. When an employee wants to talk to the SEC about the underlying facts, the SEC's interest is in making sure that that communication is not impeded.

But this still leaves room for a company to conduct a privileged confidential investigation in which it attempts to determine what the facts are. The company just can't say to its employees, "You can't talk about the facts with anyone else."

This ultimately points towards companies having a strong internal reporting and compliance system that is well known to employees and credible. That's the best and appropriate way to encourage whistle-blowers to report matters internally, rather than first running to the SEC or the government whenever there's a problem.

There also are situations in which it is advisable for companies to tell the government that it is conducting an internal investigation. Sometimes that's a very important and helpful step to take; examples include situations in which the government has already learned of the issue from a whistle-blower or otherwise. This in turn puts tremendous pressure on companies to ensure that their internal investigations are thorough and credible. Again, this relates back to the APA experience. There, it was clear that to the APA board, the most important issue to get right was publicly establishing the thoroughness and credibility of the investigation.

BBNA: Are there other new developments?

Hoffman: One growing area for internal investigations is data breaches. Target's experience illustrates that how a company handles a data breach can have a huge impact on its bottom line because it goes right to the issue of customer trust.

Within the cybersecurity sphere, the SEC's role in policing data breaches is evolving. The SEC's Enforcement Division has been conducting post-data breach investigations into whether companies' internal controls over financial reporting were sufficient as they relate to cybersecurity, and whether companies sufficiently disclosed the risks of data breaches.

In our view, it's still not clear whether the SEC's internal controls theory in this context is a valid one—other than perhaps in a situation with extreme facts—because it would require the SEC to delve into the technical details of a company's cybersecurity measures to determine if they were reasonable. That's a very tricky examination where the sophistication and frequency of cyber-attacks are so high and where all institutions in this country, including the most sophisticated government institutions such as the NSA, have been susceptible to attacks.

“In terms of internal investigations, the scope and number of government investigations into data breaches put pressure on how companies conduct internal investigations around such situations.”

In terms of internal investigations, the scope and number of government investigations into data breaches put pressure on how companies conduct internal investigations around such situations.

Just as in any other white-collar investigation, it is important that the forensics investigation into a data

² *In re Kellogg Brown & Root Inc.* (13 CARE 1798, 8/14/15).

breach is conducted with an eye towards protecting the attorney-client privilege and gaining a thorough knowledge of what actually happened.

One thing that's unique about cybersecurity internal investigations is that it is very common that the facts remain cloudy no matter how good your investigation is. One important part of the investigation relates to the company's internal security measures and its response to the attack. But equally important is trying to understand the attack itself, which not infrequently is a sophisticated criminal act conducted by a person or entity in an unknown foreign location who anticipated that their actions would be scrutinized by experienced forensic investigators. It's often difficult to figure out not only who did the act, but how the act was done, and sometimes even whether it was successful. For in-

stance, it's quite common to be uncertain about whether the hackers were able to exfiltrate data from the network, either because they hid their tracks or just because of the way the forensics data would show or not show an exit from the system.

In addition, data breaches rarely remain private. Accordingly, there is pressure for companies to think about crisis management and communications earlier in the process than in other more typical internal investigations. That in turn requires careful coordination between the company, outside counsel, and communications advisers to ensure that the legal, regulatory, and communications issues are being discussed together, and that these discussions preserve the attorney-client privilege.