Conducting Ethical Corporate Investigations

CONDUCTING ETHICAL CORPORATE INVESTIGATIONS

Anyone looking for a step-by-step approach to conducting lawful corporate investigations can steal some ideas from the Association of Corporate Counsel.

The ACC presented a panel discussion on internal investigations during its annual conference in Boston last week, and posed the following hypothetical: One of the company's office managers has received an anonymous e-mail, where the writer claims to have compromised the salary and bonus information of several executives. The writer also claims to have stolen proprietary software from the company, whose customers are mostly manufacturers, and plans to give it to a competitor.

You, the general counsel, must investigate. How do you proceed?First, said Marcia Narine, deputy general counsel and vice president of global compliance and business standards of Ryder System, is to confirm whether the information—in this case, the salary data or the software the writer mentioned—is accurate. Once you confirm that the threat appears real, the next step is to assemble a small team to help the investigation. Your first call should be to outside counsel, the second to the chair of the audit committee, Narine advised.

As to bringing other internal employees into the investigation, proceed with caution. John Lewis, senior managing litigation counsel for Coca-Cola Co., said general counsels must consider "the architecture of the case" before deciding who can be trusted for help.

For example, who would have had access to that salary data in the first place? It could be anybody from the IT, payroll, or human resources departments, Narine said. "You have to be relatively suspicious."

"THE COMPANY OWNS THE INFORMATION INSIDE THE EMPLOYEE'S HEAD AND HAS A RIGHT TO KNOW IT AND TO IMPOSE CONSEQUENCES IF THE EMPLOYEE DOESN'T COMPLY."

—John Lewis,

Senior Managing Litigation Counsel,

Coca-Cola Co.

In addition, be prepared to answer questions employees might ask (such as how the perpetrator obtained the data) before alerting them to the existence of the investigation—because once they

know about it, Narine warned, the company is taking the risk that one of them will report it to regulators.

Ralph Martin, a former district attorney in Massachusetts and now managing partner at the Bingham Consulting Group, did quip that regulators aren't "twiddling their thumbs" looking for investigations to launch; they already have much to do and generally want to take a case only when others have done the preliminary work. In this particular case, he said, the e-mail alone did not contain enough information to spark a regulatory probe.

Maintaining Control

Handling investigations internally, rather than notifying regulators, has other advantages. Foremost, since you already know the organization, you can identify where to start gathering evidence much more discreetly, determine the true severity of the threat, and pinpoint where the risk exposure exists, Martin said.

Contrast that efficiency to the time regulators would spend simply getting acquainted with your enterprise—"and that is purely advisory on your part, because you don't control it," Martin said. "Once you go to the authorities, you give up control."

Also remember that some situations do call for immediate regulatory attention: if someone's life is in danger; if valuable assets are lost; if certain laws or regulation, or even internal corporate policies, require immediate reporting.

Lewis noted that the Sarbanes-Oxley Act does give companies the ability to launch investigations quietly, by using SOX audits as an excuse to check internal controls. For example, a SOX audit can review how shared financial resources work, who codes them, and who has access to that data. This act of "sleuthing" can eventually lead to those individuals, resources, and geographies that will narrow your investigative search, he said.

Expense reports are another lucrative area for investigation. Compare employees' reports to records from vendors or customers to find any disparities, Martin said. Also watch for suspicious behavior, such as two employees expensing a company lunch when there is no business reason for it—those can be the sort of events where data is transferred from one computer to another, Narine said. "You never know how these things are going to work out."

Companies can also search numerous public records, such as court judgments, debt and bankruptcy filings, and new business registrations. Personal credit reports are not on that list, Narine said, but they aren't always helpful anyway; thieves can still have good credit.

Do be wary of the rules of electronic communication. If you're going to conduct a search of employee data, the company must have a policy that clearly states the employee has no expectation of privacy in workplace communications, experts say.

Sooner or later, however, most serious internal investigations eventually are passed along to regulators; once that happens, the company has a new level of complexity to handle. Lewis's advice: "When you notify regulators, you have to assume you're going public."
That means the small team that did the original investigation should be prepared for media scrutiny, so the company must, in turn, prepare that team. For example, Narine said, the corporate communications department should be able to supply the team with official statements.

Conflict International Limited is a London detective agency specialising in Surveillance and Private and Corporate Investigations, providing a bespoke private detective service for firms, banks, companies and private individuals

---

- Bugs in the Boardroom
- How Vulnerable Is Your Company to Cybercrime?