



COMPANIES

Early lesson from NCI breach: Double check financial oversight

- By Mark Hoover
- Feb 06, 2017

In late January, NCI Inc. accused its controller of **embezzling \$18 million over the last six years.**

The news rocked the federal contracting community and raised the question of how should companies react when something like this happens to them and what steps should they be taking to prevent this kind of breach in the first place.

First, companies should have a sound internal investigation policy that sets out how the investigation will be conducted, who it will be reported to, and what steps will be taken, said Bob Tompkins, partner, Holland and Knight.

“In a case like [NCI’s], there are a host of different notice and reporting obligations that the company will have in addition to any internal requirements they have set,” he said.

If the company is public, it must report the breach within a certain amount of days, said Lexy Kessler, lead partner, Government Contract Services Group, at Aronson LLC.

“If it is a public company, I would highly recommend that it is a third party forensics team that comes in with attorneys to understand the landscape of what you are doing, [a team] who understands you have investors that you’re reporting to,” Kessler said.

Recovery can be a long and difficult process.

“The first step is to undertake a full assessment of what happened, both to show that the company is being responsible but also to avoid further unpleasant surprises,” Tompkins said.

In light of any breach, companies should be taking a look at their internal controls.

There are a number of examples of how companies can strengthen their internal controls, said Timothy Belevetz, partner, Holland and Knight. One example is segregating duties with respect to the custody of assets. This way, no single individual should be in a position to both commit and conceal the fraud, Belevetz said.

Another example is to review and authorize expense reimbursements. “There should be a requirement to provide supporting documentation,” he said.

A third example is the reconciliation of bank accounts, Belevetz said. "This identifies any discrepancies between the company's cash balance according to its balance sheet and its bank statements. Again, there should be a separation of powers. Those who sign the checks or authorize electronic payments should not be those who do the reconciliations," he said.

Other examples include a fraud hotline, where employees can report misconduct anonymously, having an independent and empowered audit committee whose role is to direct, monitor and evaluate internal auditors, and conducting periodic fraud risk assessments, Belevetz said.

In the case of embezzlement, the company is in a tricky situation, Tompkins said.

The company "would be well served to affirmatively reach out to law enforcement," he said, as it is the victim; however, the alleged perpetrator was acting as the company's agent, so the company must draw a sharp line between itself and the bad actors, he said.

With any crisis, companies must investigate how it occurred. Unfortunately, in today's technology environment, it is near impossible to catch every potential problem, Kessler said. That said, she recommends that companies learn everything they can about a breach and put into place a corrective action. Then, communicate that to everyone who needs to know—lenders, investors, the board of directors and employees.

In the case of embezzlement, sometimes government contractors will have to reimburse the government for overcharges; however, this is only the case with cost-reimbursable contracts, Kessler said.

Obviously, the best cure to this kind of problem is prevention. Most of the time, breaches like this one are often discovered during a financial audit, Tompkins said.

"Other times, it comes about in a more organic fashion where behavior of the culpable individual or individuals suggests that there is something amiss, and increasingly, we are seeing more of that as companies begin to adopt and embrace insider threat programs," he said.

Companies that require security clearances are quick to embrace these types of programs, Tompkins said, but he is seeing more companies that do not require security clearances embrace the programs as well.

Kessler wondered at a situation that would cause a top ranking employee to embezzle money. "When life brings you a turn you do not expect, it can be a matter of survival, so to speak," she said.

So, too, companies should be aware of their employees and any behavior changes that occur—those changes might be the tip off that there is a problem, she said.

About the Author


Mark Hoover is a senior staff writer with Washington Technology. You can contact him at mhoover@washingtontechnology.com, or connect with him on Twitter at [@mhooverWT](https://twitter.com/mhooverWT).

1105 Media, Inc.

8609 Westwood Center Drive, Suite 500

Vienna, VA 22182-2215 703-876-5100 Insider Customer Service 800-353-9118 or

[email](#)

 PUBLIC SECTOR
MEDIA GROUP © 2017 1105 Media, Inc.