Tim Janes, *vice president and CSO, CapitalOne, and member of the Security Executive Council*

Anthony Heredia, *vice president of Corporate Risk and Responsibility, Target, and member of the Security Executive Council*

Richard A. Lefler, *Dean of Emeritus Faculty for the Security Executive Council and former CSO, American Express*

Park Dietz, M.D., Ph.D., *President, Threat Assessment Group Inc.*

Question: How can I prevent, detect, or respond to insider theft or fraud?

In this economic time, we cannot be comfortable simply using the "standard" fraud detection solutions that have always worked. In all industries, there are traditional areas commonly monitored for fraud such as Travel and Expense programs, general ledger issues, and — specific to financial services — areas such as teller issues and credit card fraud. While all of these areas continue to be important, it is just not good enough anymore to consider only the traditional business areas and typical fraud indicators.

For example, given decreases in consumer demand and the tightening credit market, additional focus might be given to sales programs. When employees make a good percentage of their wage from productivity and performance incentives, there is potential for them to manipulate sales data and processes to "close the deal."

Not many years ago, technology focused primarily on transactional indicators which were limited to fairly specific anomalies. There is technology available now that can help us look for irregularities, and control breakdowns and potential fraud in a wider range of areas. Some of the technology looks at a greater range of data on more platforms. Using this technology in the right way can provide a security or investigations function with much better visibility into more business areas.

Most of our organizations are feeling immense earnings pressure and are reducing capital and expense budgets to keep pace with slowing revenues, so it is likely that our ability to invest in new technologies focused on insider fraud will be significantly diminished for some time.

One often overlooked strategy to address this rising threat is leveraging all of the effort that will inevitably go into the increased scrutiny of expense reports, accounts payable and other areas traditionally ripe for fraud and abuse. Scrutiny will be heightened because expense managers are under pressure to reduce current spending and build reduced budgets for the future, so why not take this opportunity to help your business partners understand the risk for insider fraud, the effect it can have on an already pressured company, and what they should do if they come across something that looks suspicious?

Working with internal audit, payroll and accounts payable, and budget managers enables you to leverage their systems, processes and knowledge. It also provides a great opportunity to deepen your relationships with key people throughout the organization and reinforce your deep understanding of the business and its key value drivers — factors that will pay steep dividends when business finally gets back to "normal."

Overseeing the investigation of internal theft and fraud, I learned to focus on three key elements: continuous process improvement (CPI), cross-functional coordination and constant training and improvement in technology and detection tools.

CPI requires us to consider the result of each investigation and examine what we learned. Is this investigation likely based on a singular act, or is there an opportunity to take key elements and probe the system for similar cases? Can we move the investigative learning into proactive system monitoring? Can Audit add this issue to their business unit reviews? Can we add comments to the company code of conduct enhancements to seek to prevent this problem?

Coordinating with other business units is also important. Individual business units are often too lean to allow one department to conduct oversight for an investigation. A team usually consists of HR, Employment Law, Audit, and business management two levels above the problem. The team does not direct the investigation; they look at the results of the investigations and make recommendations.

Internal fraud investigations can vary from simple theft to complex financial manipulation strategies. The CSO must constantly invest in training and the use of proactive technology.

An important strategy for avoiding misconduct by insiders — theft, fraud, violence and more — is to hire people of good character. This was easier in the days of pre-employment psychological testing and when prior employers were willing to provide negative information. Today, the best substitutes are (a) sophisticated interviewing by staffing specialists or managers trained in spotting psychopaths and other trouble makers; and (b) interviews with developed sources — not the people suggested by the applicant, but others whom those people suggest.

Every employee could help detect misconduct, yet people are unlikely to report their peers unless they have an incentive to do so — such as bonuses for teams or locations that outperform others in reducing theft or fraud. This should be particularly easy to implement for retail shrinkage or workers compensation fraud, where good cost data already exist. I would suggest starting in the worst-hit locations.

When goods or equipment are being stolen before they even reach inventory, you might consider working with suppliers to implant GPS tracking devices or chips that can be tracked in high-value merchandise before it is delivered. Even if the devices are detected by employees who accept delivery of the products, the net result should be deterrence of the theft of similar merchandise.

NEXT MONTH'S QUESTION: What can I do to ensure that my supply chain is adequately protected?

For more information about the Security Executive Council, please visit www.securityexecutivecouncil.com/?sourceCode=std.