SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Investigations >

Early Fraud Detection: The Secret to Security ROI?

By the Security Executive Council

What if, by offering a particular service, Corporate Security could show a level of loss prevention or recovery that dwarfed its cost? It would be the ROI Holy Grail a lot of security leaders have spent their careers wishing for. But does it exist?

Some believe it could, in the form of early detection of internal fraud.

Internal or occupational fraud - "fraud committed by individuals against the organizations that employ them," as defined by the Association for Certified Fraud Examiners (ACFE), can take many forms, from asset misappropriation to corruption to falsifying financial reports. It can be perpetrated by staff or middle or upper management, alone or in collusion with contractors or other employees. More than 40% of cases are uncovered by tips, according to the ACFE, but by the time a tip comes in, much of the damage may already be done. Early detection could significantly decrease loss and increase recovery.

There is evidence that many companies are losing significant resources to internal fraud without even realizing it, or without recognizing the scale of the loss. In its 2020 Report to the Nations, the ACFE estimates that organizations lose 5% of revenue to internal fraud each year. In a company with $1 billion in revenue, that would equate to $500 million in loss annually.

Because fraud is an act of malicious intent against the organization – a deception (sometimes criminal) intended to result in personal financial gain for the perpetrator – Corporate Security could be accountable for detecting and mitigating the risk. But because of the variety of ways internal fraud is conducted, other functions may have authority over detecting and recovering from it as well, such as Audit, Legal, HR, and Finance.

According to the SEC's 2021 Corporate Security Organizational Structure, Cost of Services and Staffing Benchmark, the average security budget represents 0.115% of revenue. That means if a company loses even 2.5% revenue to internal fraud, and if Corporate Security does shoulder the responsibility for early detection, a conservative estimate could still show security netting a return of 20 times the organization's total investment in the function.

Despite this potential, the ACFE's 5% loss estimate, from its 2020 Global Study on Occupational Fraud and Abuse, hasn't changed much from study to study. Either fraud incidence and cost are outpacing mitigation and recovery, or companies overall aren't doing much to combat occupational fraud loss. But why?

They don't envision where it could be happening.

Some organizations focus on travel and entertainment expenses and company purchasing cards as the only places rife for internal fraud. Those are common problem areas, but unfortunately, occupational fraud happens much more broadly. It occurs within all functions that deal with payment or transaction. Here are a few examples we've seen.

A contractor and an engineer collude to overcharge the company for their service. When the payment comes in, they split the difference.

A salesperson sells a client an endcap promotion for one of their products. The salesperson never puts up the endcap, and since he or she is the party responsible for verifying the promo is in place, the client is none the wiser. This can be done by one person or in collusion between a sales representative and a store manager, for instance.

Existing employees use false names to bid for contracts for their employers and rig the bids to get themselves the contracts.

Of course, there are also the high-profile, extremely costly financial statement fraud cases we see in the news, like Enron and Lehman Brothers.

They don't believe it's happening to them.

As is so often the case in security, "undetected fraud loss" leaves us trying to prove a negative. It could be argued that if fraud is undetected, it may be because it isn't there at all, in which case efforts to stop it waste resources. And if the fraud is there, what if that 5% number is too high? It is just an estimate, after all.

This is a legitimate argument. If early detection would mean a drastic increase in man hours or technology and a requisite increase in expenditure, it makes sense to pause and consider whether an estimate – one that hasn't been proven to apply to your organization specifically -- justifies the cost.

The logical response would be not to ignore the potential threat but to test for vulnerability, or to have someone skilled in this arena work together with you to examine your risk. Could an early detection program be instituted temporarily to see what the impact might be? One of our subject matter experts established and ran a proactive investigative unit for his company (a Fortune 500 financial company) whose remit included early fraud detection. Initially established on a "try and see" basis, the group became a critical and enduring part of the company's fraud prevention and detection strategy, regularly weeding out inappropriate or malicious acts by insiders and significantly reducing fraud losses.

Each function assumes someone else is already dealing with it.

Find out where the responsibility for recovering internal fraud losses should sit in your organization. Is it Audit? Is it Security's role? HR? Is each function responsible for monitoring for fraud on its own accounts? Who is looking for anomalies?

Chances are, it will be hard to find an answer to these questions. Confusion over who owns investigations is common in many organizations. One SEC analysis identified up to 67 types of corporate investigations, with accountability spread out over up to 13 different business functions.

If you can pinpoint a responsible party (or parties), ask them how much money has been recovered, how many people have been under disciplinary action, how many terminated, and how many prosecuted.

If you can't find anyone responsible for fraud detection, or if losses are being recovered but perpetrators are not being disciplined or prosecuted appropriately, then the job isn't getting done, and your company is losing money to fraud because of it.

Are you, the security leader, uniquely positioned to oversee an investigative function for early fraud detection that spans all potentially impacted departments by facilitating role definition, organizational responsibility, and priorities? Centralized investigations, including occupational fraud investigations, could eliminate redundancies and ensure that those doing the investigating are properly trained to do so. A coordinated effort helmed by trained investigators could catch internal fraudsters early in the scheme, saving the company more significant loss.

They don't know what to do about it.

Internal fraud is complex, and those who perpetrate it generally have the access and insider knowledge to cover their tracks. This makes discovering it particularly challenging, but not impossible. According to the Handbook of Statistical Analysis and Data Mining Applications by Robert Nisbet, "The basic approach to fraud detection with an analytic model is to identify possible predictors of fraud associated with known fraudsters and their actions in the past. The most powerful fraud models (like the most powerful customer response models) are built on historical data."

If the organization has detected fraud by employees in the past, what were the markers of those schemes? Go through transactional data and records to look for anomalies that were missed. Could monitoring for similar anomalies trigger an earlier investigation in the future? One example of an anomaly could be an employee's address on file with payroll that appears in another payments database with an alternate name. Running a comparison between databases could uncover employees using fake identities to collect fraudulent contract payments.

Investigators can use root cause analysis to help detect the motives and opportunities for fraud. Again, research and historical data can help identify potential red flags. External and demographic data can also be rolled into this effort. The ACFE lists living beyond one's means and having existing financial trouble as notable red flags, along with an unusually close association with a vendor or customer and an unwillingness to share duties. What processes and procedures can be put in place to monitor for red flags in the future?

As noted earlier, almost half of detected internal fraud cases are uncovered by tips. Ensure your organization offers multiple methods for anonymous tip reporting, and assign a group or individual to follow up.

Further considerations

As a corporate security leader, ask yourself what your function is doing to protect against fraud and detect it early. It's important to engage a cross-functional group that looks at the issue of identifying fraud proactively. Partner with Finance and Audit to show the value of fraud monitoring and create a realistic process to address it.

The SEC can help companies interested in exploring early fraud detection by analyzing the opportunity (is it worth it for you?), exploring the viability of a program, helping create historical fraud profiles, helping identify cross-functional team members, and facilitating internal collaboration. We can also help to run a pilot program to determine the scale of the internal fraud threat in your organization.

Early fraud detection may not be the universal Holy Grail of ROI for every company. But it has the potential to move Security from a cost center to net or profit and to save significant money for the organization. It's wise to take a look at where your company's exposures may be.

Visit the Security Executive Council web site to view more resources in the Program Best Practices: Investigations series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

