SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Investigations >

How Proactive Investigations Can Boost the Bottom Line

By the Security Executive Council

Organizations can incur criminal loss through many avenues – organized crime, theft and diversion, intellectual property loss, myriad types of internal and external fraud involving insurance, employee benefits, misappropriation, kickbacks, and more. Each of these loss avenues may be managed by a different function in the company, which is why there is seldom a single point of oversight for loss recovery and investigations.

Often, losses of all types are discovered by accident, through tips, or when the company is informed of the criminal act by police, and by then, a significant portion of the loss is likely unrecoverable.

Some SEC faculty (former CSO subject matter experts) and Tier 1 clients have addressed these issues by successfully employing proactive investigation methods to detect loss much earlier, recovering assets and making a notable bottom-line impact for their companies. They discussed these efforts in the December 2021 Security State of the Industry: Proactive Loss and Anomaly Detection.

Phone Charge Reimbursement

Proactive detection can take many different forms, from document review to perpetual ongoing monitoring. It doesn't necessarily require huge data systems. Bob Hayes, SEC Managing Director, related an experience in the late 1990s when his company, Georgia Pacific, was spending $3 million to reimburse employees for business-related cell phone charges including roaming and long distance. His group reviewed the reimbursement claims, actively investigating around 200, and discovered both unintentional and intentional errant claims. The investigation

led the company to enact spending limits and renegotiate contracts, ***reducing risk exposure by 20%.*** All this was done without the use of big data systems.

Insider Theft of Data and Information

Another presenter described approaching company executives with a plan to curb loss of valuable information to employees who leave the company, either by choice, to work for competitors, or as part of a workforce reduction. He presented the probability that half of employees leaving to competitors take information with them, and a quarter of employees terminated do the same.

Because data-based, proactive detection of insider risk can be an expensive undertaking, and because it can be viewed as spying if it's not adequately justified, this security leader knew it could be difficult to get buy-in. So, he laid the foundation by presenting strong data and proposing an investigative program with a structure of good governance, policy, standards, and well documented processes. It was important to begin with a clear formula to identify the value of information being lost, to present proof and solid documentation, and to lay out how the results would be used.

The program has resulted in significant financial return on investment annually, and because it is so well documented, this security practitioner has been able to clearly show ROI. The results have been definitive enough to justify a six-fold increase in resources for the program over two years.

Fraudulent Vendor Payments

Matt Giese, SEC Emeritus Faculty, discussed his experience using proactive methods to investigate potential vendor fraud. The company in question contracted with thousands of vendors for a spend of hundreds of millions annually. The risk exposure to vendor fraud was about 5% of annual revenue.

Matt used the vendor master file to cross-match for indicative data—including addresses, bank account numbers, phone numbers—looking for duplicates and for potential matches to company employees who may be falsely representing themselves or unethically doing business separately as vendors. The investigation ***uncovered and resolved numerous bogus vendor contracts and fraudulent vendor payments***.

Supply Chain Diversion

Francis D'Addario, SEC Emeritus Faculty, began proactive investigations at Starbucks before it was a multi-billion-dollar company. He applied exception-based reporting to the supply chain and discovered that there was a loss of ***$10 million in sales*** because of 1 million pounds of coffee going missing between shipment and delivery. These were declared as mis-ships – the retail location claimed it didn't receive the items, so more would be sent to replace what had gone missing. However, investigators determined that the loss was occurring at the retail end, so they started calling stores. The very first investigator discovered inventory that was not actually missing. Certain employees were diverting the products to start competing retail outlets with Starbucks coffee.

Francis made sure to quantify the recovery and prevention of loss to executives so they could easily see the bottom-line impact of the investigation. Proactive investigation, according to Francis, is a path to growth.

Computer Reimbursement Benefit

Another experience shared by Matt Giese: the investigation of misuse of a computer reimbursement benefit provided by Fidelity during his tenure there. The benefit reimbursed employees for 20% of new computer purchases every three years, up to $2,000. Giese's team saw the potential for fraudulent claims and identified the employees who had requested the maximum reimbursement allowed, then used the submitted receipt information to check the status of the sales with the stores that had sold the computers. They quickly discovered employees who had submitted the reimbursement requests, then cancelled or returned their orders, pocketing the money.

When these results were taken to HR and Legal, it was decided to continue with the investigations and to terminate employees who had effectively stolen from the company. The full investigation uncovered hundreds who had abused the program ***for hundreds of thousands of dollars*** in loss, which could then be recouped.

Success Factors

While there are many ways to conduct proactive investigations, here are some common success factors our speakers shared:

- To be a success, you must show good governance, policy, standards, and process documentation, as well as strong metrics and reporting. High-quality, informative metrics are the best way to secure funding for ongoing operations.

- Investigative techniques and processes that lead to common success generally aren't used in investigations run by non-security personnel, possibly because security personnel are more likely to have law and investigations backgrounds. A Security investigative team can take the lead in areas of investigative confusion and be proactive.
- Even sophisticated, well-funded investigative programs often lack the time to engage in proactive detection. Dedicated resources are critical for concentrated consideration of risk exposure.
- If your proactive detection program will incorporate sophisticated data-based intelligence techniques, it is important to have trained data analysts on board. Effectiveness will be limited if these techniques are executed by personnel without the appropriate training.
- Alignment with corporate culture is important, as is careful communication. Without proper contextualization, proactive detection can be perceived as spying.
- Multi-functional engagement is also critical. Include Legal, HR, Audit, Risk and Compliance. If Security steers the ship, it's important to communicate that the work and the trust is shared.

Next Steps

Security State of the Industry quarterly presentations are just one of the benefits of becoming an SEC Tier 1 client. For more information, contact us at contact@secleader.com.

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/