SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Investigations >

New Developments in Proactive Loss and Anomaly Detection

By the Security Executive Council

Companies lose money in a diversity of ways, but whether the loss is via theft, fraud, poor management, or error, the longer it takes to detect it, the more costly it will be.

In the March 2023 Security State of the Industry: New Developments in Proactive Loss and Anomaly Detection, Garry Birkhofer, SEC Subject Matter Expert, Asset Protection and Anomaly Detection, along with a Director of Corporate Security and Business Continuity at an international supplier of industrial machinery and equipment, joined Bob Hayes, Kathleen Kotwica, and Liz Lancaster from the SEC to discuss how business analytics tools can be used to detect anomalies and stop loss before it compounds.

Here are some highlights of the conversation.

Traditional vs Proactive Investigation

Traditional investigations programs are typically reactive. In the traditional model, loss isn't investigated until it's reported, which could be long after the loss occurred or began to occur.

Proactive investigations analyze data to discover correlating factors that may indicate loss, allowing investigation to commence after a loss has occurred but before a loss has been reported.
The SEC has previously shared cases in which proactive investigations boosted organizations' bottom lines, According to the National Retail Federation, shrink accounted for $94.5 billion in losses to U.S. retailers in 2002. Yet many retailers conduct only one annual inventory. They may find loss that occurred – or began to occur - 11 months prior, and over that 11 months, accounting and system errors will have continued, and exploited vulnerabilities to theft and fraud remained open to continued abuse.

some of which incorporated sophisticated technology, and others that relied on boots on the ground. Each of the cases showed unmistakable ROI; for example:

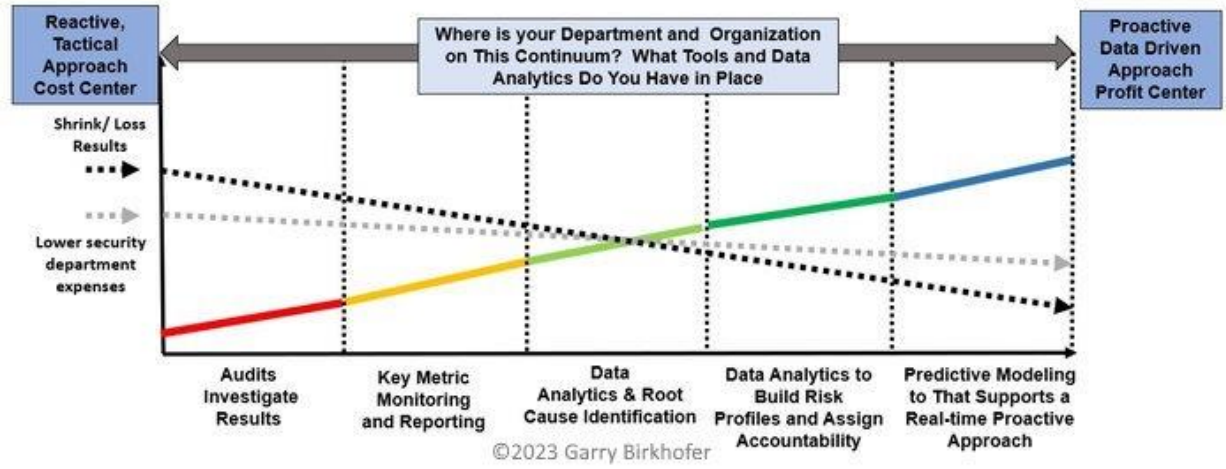
- A 20% reduction in risk exposure.
- Significant enough financial return to justify a six-fold increase in resources for the program over two years.
- Discovery of the root cause and partial recovery of $10 million loss.

While any proactive loss detection program has great potential to add value, programs that don't incorporate sophisticated analytic technology can be limited in what they can discover and how long that can take. They aren't always able to cross-reference red flags across the organization, and if they do, the time commitment can be significant.

[Research by the Association of Corporate Fraud Examiners] found that in 2022, a typical occupational fraud case causes a loss of $8,200 per month and goes on for about 12 months before it's detected, which happens most often when another employee tips off the organization to the scheme. That's a typical $98,400 annual loss per case.

More from the SEC on the business case for early fraud detection: [Early Fraud Detection: The Secret to Security ROI?]

Results Achieved: As Companies Becomes More Proactive, Losses and Expenses Decline



How Data Analysis Platforms Can Enable Proactive Investigations

The speakers shared their experience with the Power BI data visualization platform and KNime tool. (Other tools with similar capabilities in the business intelligence and data analytics space

include Tableau, Qlik Sense, Klipfolio, Looker, Zoho Analytics, and Domo.) The process enhanced their ability to:

- Define loss, how loss is measured, and who is responsible for follow-through.
- Identify the root cause of loss by examining operational metrics, inventory accuracy, process execution, monthly accounting, safety metrics, and other data that can indicate gaps in execution or can pinpoint bad actors, and cross-referencing data across the enterprise to connect the dots.
- Categorize data to identify trends that point to potential problems. For instance, inventory adjustments can be filtered by location or even by employee or item.
- Create a risk index that can be easily deciphered and accessed by the executive team.
- Focus resources on areas whose data shows they are skewing towards higher risk.

Speakers cited a significant investigation whereby a contractor on new construction projects was shorting the amount of asphalt poured in new construction sites. The contractor had pocketed hundreds of thousands of dollars doing this over several years until predictive factors were brought into play. Correlating loss to extrinsic data factors like repair information and insurance claims allowed the company to cut off the contractor and stem further loss.

Bob Hayes noted that proactive investigative processes could also be applied to product warranty claims, damage claims, procurement, expense accounts, travel, insider trading, and more.

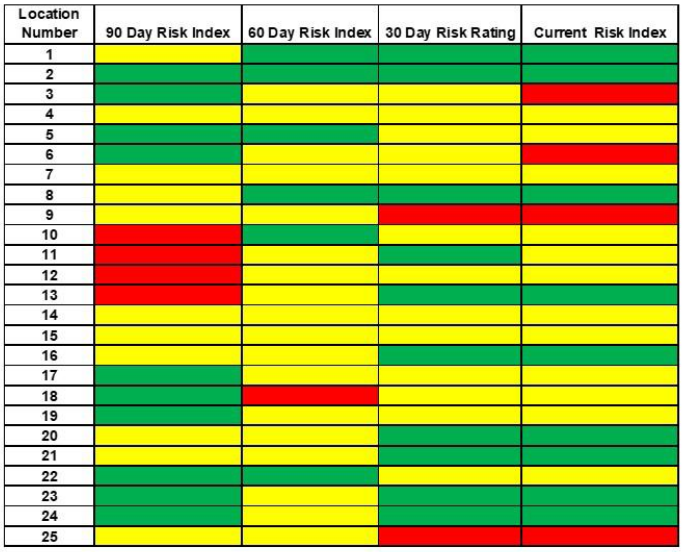
How It Works

Birkhofer outlined the process of implementing an analytics platform for proactive investigation. There is an upfront investment in time, and business and risk owners must be engaged from the beginning.

- Identify leadership's risk priorities.
- Determine dependent variables and metrics that correlate to loss.
- Collect and prepare data, pulled from existing company databases.
- Create a master spreadsheet for analytics and profiling.
- Determine if correlations appear and validate initial hypotheses.
- Establish thresholds, weight metrics, and use those to calculate a risk index.

Sample Predictive Model Summary Screen Shot

- This dashboard view can be company-wide, regional, district, and for a specific location
- This initial Risk Index view of the dashboard that shows trending to focus on locations that went from green to yellow or yellow to red over the **last 120 days**
- Then by clicking on a specific location the detailed dashboard would highlight what metrics changed that caused the change in the Risk Index
- This level of detail by metric helps to target key root causes areas to investigate



Location Number	90 Day Risk Index	60 Day Risk Index	30 Day Risk Rating	Current Risk Index
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				

Silos Remain the Challenge

Because this type of proactive investigations model is data-based, it isn't difficult to quantify or articulate its value to executives. The challenging part is, according to the Director of Security, "getting engagement from all the disparate business units when you're calling their baby ugly, so to speak."

Because there are so many ways for assets, including money, to leave a company, all functions have some responsibility for areas in which loss may be occurring. And accessing companywide data for analysis requires active partnership with the functions that maintain that data.

"Bringing our partners along becomes the art and challenge for us," said the Director of Security. "And doing that is, I think, strategically, no different than any other change management. It's identifying the right partners, taking them hand in hand, working together and spreading the sphere of influence out from us."

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/