FEATURE

Fighting Fraud

Considering Data Analytics

Occupational fraud, e.g., internal theft, employee fraud and asset misappropriation, plagues enterprises of all sizes. The perpetrators work for and among their victims and are using greater and more sophisticated means for hiding their deceptive practices.

Occupational fraud news headlines are widely circulated and very familiar to enterprises. Examples include:[1]

- A government mailroom employee skimmed more than US$2 million in taxpayer refund checks that had been returned by the post office for bad addresses.
- A bookkeeping employee stole more than US$200,000 of cash payments but still posted the transactions to the enterprise accounts-receivable detail.

- A purchasing agent for a major enterprise established a vendor file in his wife's maiden name, then approved more than US$1 million in enterprise payments to her.
- The chief executive officer (CEO) of a small nonprofit agency stole US$35,000 from the agency by submitting check requests that were made payable to outside bank accounts that the CEO controlled.

Although 2018 marked the seventh consecutive year that white-collar crime prosecutions fell in the United States,[2] the US Federal Bureau of Investigation (FBI) reports that these crimes continue to cost the country more than US$300 billion annually.[3]

It may seem like enterprises are making little progress against occupational fraud. In 2014, enterprises lost approximately five percent of their annual revenue to fraud; in 2018, the estimate remained at five percent.[4] Yet a closer look at these numbers suggests that data analytics is helping enterprises fight back. Fraud cases studied revealed that enterprises that used data analytics to combat fraud experienced 58 percent faster detection and 52 percent fewer losses than enterprises that did not use data analytics for the same purpose.[5]

Fraud-specific data analytics uses analytic technology, fraud analytic techniques and human

Chris Errington, CRCMP, CSPO, GRCP
Is a senior communications specialist, internal audit at Nielsen Global Media. He oversees the writing and editing of numerous documents for the department and industry-related articles for publication and leads critical research initiatives.

Kevin M. Alvero, CISA, CFE
Is senior vice president of internal audit, compliance and governance at Nielsen Global Media. He leads the internal quality audit program and industry standards compliance initiatives, spanning the company's Global Media products and services.

Wade Cassels, CISA, CCSA
Is senior operational auditor, internal audit at Nielsen Global Media. He supports Nielsen's IT general controls external audit engagement and the audit reporting and communications functions for the department.

interaction to successfully detect and deter improper transactions either before or after they occur. Data analytics is not a panacea against internal fraud. Tips from aware individuals, such as those received via employee hotlines, remain the most common method of detecting internal fraudulent activity. For data analytics to be able to help enterprises combat fraud, users (e.g., internal audit, security, human resources and IT) must have at least a fundamental understanding of occupational fraud to understand the connection between suspicious transactions and fraud. For example, in cases of internal fraud and abuse, people committing illegal acts rarely limit themselves to a single type of fraud; instead, they take advantage of employers by stealing whenever they can. This information is critical to enterprises seeking to accurately quantify losses from fraudulent activity.

> “DATA ANALYTICS CANNOT REPLACE THE NEED FOR AN ETHICAL CULTURE, AN UNDERSTANDING OF FRAUD AND A SOUND SYSTEM OF INTERNAL CONTROLS.”

At the same time, those tasked with mitigating internal fraud must understand the fraud warning signs of employee behavior, such as living beyond one's means. Although these warning signs may not be part of transaction monitoring, they can be key clues to use along with data analytics to paint a clearer picture of where fraud may be occurring and what additional investigation may be most prudent.

Data analytics cannot replace the need for an ethical culture, an understanding of fraud and a sound system of internal controls. However, by combining internal controls, such as data analytics, with personnel insights, enterprises can better and more proactively deter and prevent occupational fraud.

Fraud's Impact on Enterprises

Occupational fraud assumes many forms, which can be organized into three categories:[6]

- **Asset misappropriation**—Employees steal or misuse enterprise resources. This type of fraud is the most common, but least costly to enterprises, occurring in more than 89 percent of reported cases and resulting in a median loss of US$114,000.
- **Corruption schemes**—Employees misuse their influence in a business transaction to gain benefit and violate their duty to their employer. This type of fraud is found in approximately 38 percent of occupational fraud cases and has a median loss of US$250,000.
- **Financial statement fraud**—Employees intentionally cause a misstatement or omission of information in enterprise financial reports. This type of fraud is found in 10 percent of reported cases and is the most costly to enterprises, averaging US$800,000 per scheme.

The Switch to Automation

Traditionally, enterprises have relied on human observation and internal control systems to detect fraudulent activities. However, these detection practices often have weaknesses that can be exploited. As enterprises turn to IT systems to store and manage business data and support business processes, the “level of human interaction has been reduced to a greater extent which in turn becomes the main reason for fraud to take place in an organization.”[7] In today's technology-driven world, where data and transaction volume are growing exponentially, enterprises of all sizes, revenue and industries must remain vigilant. Failure to do so can expose the enterprise to catastrophic risk in terms of lost revenue, fines or other penalties, and reputational damage.

Data analytics provides enterprises with the opportunity to identify root issues and trends and produce detailed results. Due to overwhelming

numbers of daily organizational transactions, without automation, it is increasingly difficult to scrutinize enough individual transactions to be able to identify issues and trends. This lack of scrutiny allows individuals to commit fraud and materially impact financial results.

Technology enables enterprises to analyze, compare and log data at the individual transaction level, making it much more difficult for personnel to painstakingly cover their fraudulent activities. Technology equips enterprises with the support necessary to eliminate fraud before it occurs or well before it negatively impacts the enterprise bottom line. Announcing to all personnel that a data analytics program is being used to detect fraud can often deter employees from beginning fraudulent activity.

Not all enterprises are equally suited to reap the benefits of data analytics in the fight against fraud. Larger and more mature enterprises tend to have clearly defined policies, control frameworks, and technical and fraud-related expertise, which impact the fraud-fighting value of data analytics. However, more enterprises can benefit from data analytics to fight fraud than are currently.

Smaller organizations (i.e., those with fewer than 100 employees) on average have fewer anti-fraud controls (e.g., data analytics, a more dedicated fraud team or fraud training) than larger organizations, making them more susceptible to fraud.[8] The median loss per incident for the smaller enterprises is double that of the larger enterprises—another compelling reason for smaller enterprises to consider fighting fraud with data analytics.

Before investing in data analytics to combat fraud, enterprises should ensure that they have the following basic elements in place:

- Information systems that can produce reliable, quality data for analysis
- Accurate risk assessment that identifies the most valuable and vulnerable enterprise assets and processes
- Understanding of the types of occupational fraud and those that pose the greatest risk to the enterprise

Without these basic elements, investment in a data analytics capability will most likely yield disappointing results, but with these elements, even enterprises with very limited resources can employ data analytics options to support antifraud efforts.

Selecting the Best Solution

A quick Internet search proves that enterprises have numerous data analytics tools from which to choose. Some websites provide interactive tools with numerous data analytics tests that help identify occupational fraud warning signs. Others provide a comprehensive list of more than 100 data analytics options. Still others provide free data analytics solutions.

Some enterprises over-invest based on their needs. In a rush to use the latest and greatest technology available, these enterprises are "opting for expensive fraud detection solutions that do not match with the company's strengths and weaknesses."[9]

> "WITH EASY-TO-USE TOOLS, QUICK DATA ANALYSIS AND THE ABILITY TO HANDLE LARGE DATA VOLUMES, DATA ANALYTICS PRODUCTS PROVIDE A LEVEL OF SECURITY THAT ENTERPRISES DESPERATELY NEED."

However, most solution providers do not offer a one-size-fits-all approach. Instead, they often provide a suite of solutions that can be tailored to most effectively fit the needs of an enterprise, especially regarding price and functionality.

With easy-to-use tools, quick data analysis and the ability to handle large data volumes, data analytics products provide a level of security that enterprises

> HOWEVER, BEFORE EMBARKING ON A DATA ANALYTICS JOURNEY, ORGANIZATIONS OF ALL TYPES AND SIZES MUST ENSURE THAT THEY UNDERSTAND THREE FUNDAMENTAL CONSIDERATIONS.

desperately need. Some solutions provide auditors with artificial intelligence (AI) and advanced algorithms that allow them to transform large amounts of data into valuable and workable insights. "Look for a solution that offers a single-stack [capability] and is powerful enough to handle even the most complex data while still being intuitive enough for less technical users."[10]

One critical question remains—especially for smaller businesses with tighter budgets: What is the cost for this added protection?

Although most data analytics providers refrain from divulging their pricing structures and, instead, require interested enterprises to complete an online form to receive a customized quote, two providers offer a glimpse into cost. The Looker Business Intelligence Platform "offers subscription pricing that ranges from $3,000 – $5,000 per month for 10 users, and $50 per month for each additional user."[11] The Tableau Creator plan "costs $70/user/month, regardless of whether the platform is deployed on site or in the cloud."[12] These examples show that data analytics solution pricing is varied and widespread.

To determine the most appropriate solution for the most suitable price, enterprises must do much of the work by proactively evaluating their own weaknesses and needs and connecting with data analytics providers.

Solution providers often highlight the benefits of added security that their tools provide as justification for this added expense. More industry leaders are agreeing.

> *Without a way to obtain, cleanse, organize and evaluate the data, the enterprise is left with a vast, chaotic pool of ones and zeroes. Data analytics (DA) coaxes order from the chaos. It helps explain patterns, which in turn help the enterprise identify… problems before they spiral out of control. DA can be relatively simple, but it can also be extraordinarily complex. Its results can be used to identify areas of key risk, fraud, errors or misuse; improve business efficiencies; verify process effectiveness; and even influence business decisions.*[13]

With a plethora of solutions from which to choose, enterprises must determine the one that best supports internal maintenance, supervision, cost, scalability and usability. Many enterprises are meeting all of these needs by collaborating with a proven data-analytics service provider. These enterprises are working to generate the greatest return on investment and ensuring that they are not going to be highlighted in the next fraud scheme news headline.

Conclusion

Occupational fraud impacts organizations of all sizes and industry types, and fraudsters are utilizing more sophisticated technological methods to conduct and conceal their fraudulent activities. At the same time, organizations are relying more heavily on their data as a source of value, including using data analytics as a tool for detecting fraud. The use of AI and machine learning as part of organizations' antifraud efforts is expected to almost triple in just the next two years.[14]

However, before embarking on a data analytics journey, organizations of all types and sizes must ensure that they understand three fundamental considerations. First, they must understand what types of fraud risk are the most likely and most impactful to their business so that investment in data analytics is pointed in the right place. Second, they must possess quality data that are complete, accurate and accessible to form the inputs for their data analysis. Finally, they must ensure that their

data analytics strategy aligns with their overall technology strategy to maximize the value and efficiency of the process and ensure that it is consistent with the organization's mission.

Given these considerations, and with a plethora of options available, virtually any organization can benefit in some way from data analytics in its fight against fraud.

Endnotes

1 Wells, J. T.; "Enemies Within," *Journal of Accountancy*, 30 November 2001, *www.journalofaccountancy.com/issues/2001/dec/enemieswithin.html*
2 TRAC Reports Inc., "White Collar Prosecutions Fall to Lowest in 20 Years," *TRACREPORTS*, 24 May 2018, *https://trac.syr.edu/tracreports/crim/514/*
3 Legal Information Institute, White-Collar Crime, Cornell Law School, Ithaca, New York, USA, *www.law.cornell.edu/wex/white-collar_crime*
4 Association of Certified Fraud Examiners Inc., *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*, 2019, *www.acfe.com/report-to-the-nations/2018/*
5 ACL, *Detecting and Preventing Fraud with Data Analytics*, Canada, 2013, *https://www.acl.com/pdfs/ACL_fraud_ebook.pdf*
6 Association of Certified Fraud Examiners Inc., *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*, 2019, *www.acfe.com/report-to-the-nations/2018/*
7 *Op cit* ACL
8 *Op cit* Association of Certified Fraud Examiners
9 EDUCBA, "Some Effective Techniques of Fraud Detection Analytics," 2019, *www.educba.com/fraud-detection-analytics/*
10 Blitz, S.; "Four Ways to Implement Data Analytics Best Practices," Sisense Inc., 24 August 2017, *www.sisense.com/blog/4-ways-implement-data-analytics-best-practices/*
11 *Ibid.*
12 Better Buys, "Looker vs. Tableau: Pricing and Features Comparison," 18 April 2018, *https://www.betterbuys.com/bi/looker-vs-tableau/*
13 ISACA®, *Data Analytics—A Practical Approach*, USA, 2011, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Data-Analytics-A-Practical-Approach.aspx*
14 Association of Certified Fraud Examiners, *Anti-Fraud Technology Benchmarking Report 2019*, *https://www.acfe.com/technology-benchmarking-report.aspx*