DETECT FRAUD AND OTHER MISCONDUCT WITH DATA ANALYTICS

BETTER DATA CAN REDUCE RISK AND LIABILITY FOR AN ORGANIZATION AND SHOW REGULATORS THAT A COMPANY TAKES ETHICS AND COMPLIANCE SERIOUSLY.

BY KELLY M. WARNER & ANDREW J. WU
APRIL 30, 2021

As the vast majority of business communications are conducted electronically — on ever-increasing platforms and applications — it is no surprise that regulators and organizations are taking more of a data-driven approach to detect and prevent employee wrongdoing.

Most importantly, regulators in the U.S. and across the world have stated they expect corporate compliance programs to include a data analytics component. In addition to being able to meet regulatory expectations, corporations are finding the focus on data analytics to be fruitful: According to a recent ACFE Report to the Nations, organizations that implemented proactive data analytics tools detected fraud 58 percent faster and experienced financial losses that were 52 percent lower than organizations that did not implement such tools.

Whether as a proactive measure to identify fraud, theft of IP, harassment and other misconduct — or as a powerful tool to aid in uncovering the depths of wrongdoing once identified — data analytics can assist in reducing risk and liability for an organization and demonstrate to regulators that a company takes ethics and compliance seriously.

THE BENEFITS OF USING DATA ANALYTICS

Analyzing data allows organizations to distill massive and bespoke information sets — such as internal and external communications, social media usage, network activity, customer interactions, cross-border transactions, financial reports and accounting records — to identify and determine the who, what, when and why of fraud and other misconduct.

Using analytics can assist organizations in identifying patterns, aberrations and sentiments that would be impossible to detect otherwise. Moreover, organizations can select data sets based on their unique priorities, needs and goals to craft tailored parameters to address the specific risk or incident at hand.

REGULATORY EXPECTATIONS

In its Guidance on Corporate Compliance Programs, the touchstone of the Department of Justice's approach to assessing corporate citizenship, the DoJ has signaled its expectation that companies implement some form of data analytics to monitor the effectiveness of their compliance programs and to detect wrongdoing. As part of its evaluation of a company's compliance program, the DoJ will look into a company's efforts to use its own data sources to "allow for timely and effective monitoring and/or testing of policies, controls and transactions."

Similarly, the U.K. Serious Fraud Office's (SFO) Guidance on Deferred Prosecution Agreements — which outlines the SFO's expectations with respect to companies desiring deferred prosecution (i.e. favorable treatment) for their misdeeds — notes that the SFO will assess proactive compliance measures the company has implemented, including "the use of data analytics to test compliance controls and behavior."

FRAUD, CONSPIRACY AND SCHEMES

According to a 2020 PwC Global Fraud Survey, 37 percent of fraud was committed by internal perpetrators; specifically, those in middle management, operations staff and senior management roles. By leveraging data analytics tools, organizations can run down potential root causes, inconsistencies or patterns that would otherwise be extraordinarily difficult to find — such as covert schemes between employees and vendors, bribery schemes with foreign officials or customers or internal expense fraud.

The use of data analytics can be especially powerful in quickly identifying any anomalies or patterns by senior management. It can be leveraged to detect subtle patterns or unique markers that would not otherwise be detected, including critical decisions made by those with certain authority. In addition, implementing data analytics can be a more neutral approach to investigating the conduct of executives. If the tool is implemented for all employees at a certain level and above, there can be less internal apprehension associated with flipping the switch. After all, while executives committed only 20 percent of occupational fraud, they caused the largest financial losses on average for organizations.

Organizations can also leverage data analytics to track and detect inconsistencies or patterns in accounting or disclosure practices. By monitoring or tracking anomalies or patterns in financial reporting, accounting records and internal audits, organizations can better position themselves to show that they are taking their reporting and accounting obligations seriously — all while demonstrating to the government that they are taking a data-driven approach to prevent wrongdoing.

In addition to expecting corporations to make use of the data available to them, the U.S. government is making use of data analytics as it pursues enforcement actions. In two recent enforcement actions, the SEC used a data-driven approach to uncover alleged accounting and disclosure violations resulting from two public companies' inaccurate reporting of quarterly earnings.

Both companies misrepresented their financial performance, which ultimately allowed them to consistently report earnings per share (EPS) that met or slightly exceeded consensus EPS estimates. The data compiled by the SEC reflected patterns showing both companies meeting or slightly exceeding consensus EPS estimates for consecutive quarters followed by substantial drops in EPS. Both of these settled actions arose from investigations generated by the SEC's "EPS Initiative," which "utilizes risk-based data analytics to uncover potential accounting and disclosure violations caused by, among other things, earnings management practices."

This suggests that other companies exhibiting similar reporting or accounting patterns may be subject to increased scrutiny by regulators, and companies should be considering what the data reveals with respect to their reporting.

INTELLECTUAL PROPERTY THEFT

The risk of IP theft remains one of the highest priorities for organizations, especially in the technology and media industries. According to a 2020 Kroll Global Fraud and Risk Report, employees and contractors were collectively responsible for more than one-third of IP theft, confirming what organizations have long known: Individuals from within an organization — and those who regularly interact with those individuals — pose a meaningful risk, and organizations should be in a position to adequately prevent and respond to such threats.

Such internal leaks pose a real risk to organizations. The Kroll report surveyed over 500 senior executives at various organizations and found the incidents that most significantly affected organizations were leaks of internal information. In particular, organizations in the financial services sector considered leaks of internal information their top priority. Organizations can implement proactive measures to detect inconsistencies, suspicious patterns or other red flags in users' data access and exfiltration.

By analyzing data from communication tools such as email and instant messaging platforms like Microsoft Teams and Slack, organizations can gain insight into the sentiment of conversations users are having and distinguish between "casual" or "business" conversations to detect anomalies or patterns in employee behavior. Such data can also illuminate potential risk factors associated with certain employees (e.g. departing executives).

Organizations can also implement data-loss-prevention tools to search for certain files leaving the organization, crunch network access logs to determine whether users' activity patterns have changed and track the frequency with which employees and competitors communicate. By implementing data analytics, an organization can demonstrate that it used reasonable measures to protect its IP, an essential element in the misappropriation of trade secrets or theft of confidential-information claims in many jurisdictions.

Lastly, data analytics can be particularly useful in forensic investigations concerning IP theft. Organizations can review departing employees' devices to identify questionable file transfer activity and evaluate whether any data was stolen or modified, including an organization's IP or other confidential or proprietary information.

HARASSMENT AND OTHER WORKPLACE ISSUES

Even with solid workplace harassment policies and training, organizations still experience risks and liability associated with employees' compliance with such policies. By using data analytics, organizations can assess the efficacy of their anti-harassment efforts and identify risky relationships and hot spots before incidents occur or continue. Such analysis can include combining survey responses from climate and pulse surveys, responses to workplace harassment training course questions, exit interview data, internal messages or emails, employee reviews or formal complaints to identify patterns or inconsistencies with respect to certain workplace issues like harassment, discrimination or hostile work environments.

For example, data analytics could reveal patterns in the composition of certain employees who file complaints — triggering events leading up to certain complaints, the relationship between job functions of the accuser and the accused or conflicts with specific department heads. If the data reveals that an organization is particularly susceptible to harassment or a hostile work environment by a specific employee or department, organizations can act quickly to take remedial measures and make appropriate adjustments to prevent brand or reputational damage. Furthermore, data analytics can be used to bolster an organization's compliance programming, which may lead to revisions to policies, training and processes.

As shown above, the DoJ is focusing on whether organizations have made adequate uses of data analytics in connection with their internal compliance measures — a strong message to all organizations moving forward that they should not just assess the data, but also make modifications as suggested by those findings. After an organization has evaluated the data and made relevant findings, organizations have an opportunity to course correct where necessary, fine-tune compliance measures and mitigate risk with more accuracy and efficiency.

Regulators not only expect data analytics, but more organizations are finding that it can be leveraged to fill in gaps, enhance efficiencies and help drive decision-making processes — which will ultimately have a lasting impact on preventative and investigate efforts.

Kelly M. Warner *is a partner at Riley Safer Holmes & Cancila LLP.*

Andrew J. Wu *is an associate at Riley Safer Holmes & Cancila LLP.*