http://www.garp.org/#!/risk_intelligence_detail/a1Z40000002w8KFEAY

The Art, Science and Technology of Conduct Risk Management

Friday, July 17, 2015, By Katherine Heires

Predictive, cognitive computing roots out bad behavior; “tone in the middle” gains sway over “tone at the top”

In 1987, Michael Jackson sang “I’m Bad” and, according to some, celebrated bad behavior. Others say the song is really about being good.

Today in the financial services industry, and in other sectors touched by scandal, there is no longer room for ambiguity: Bad behavior is not tolerated. Conduct risk is high on the regulatory agenda, as articulated recently by the Group of 7 finance ministers and the chairman of the International Organization of Securities Commissions among others. It is also increasingly prominent in corporate compliance and risk management mandates and written ever more insistently into codes of ethics.

In this environment of heightened sensitivity to the consequences of unethical or illegal conduct – along with the billions of dollars of exposure to penalties for wrongdoing and its accompanying compliance costs – have emerged fresh approaches for identifying, rooting out and even predicting bad behavior.

Two providers of risk management and surveillance technologies to the financial industry, the long-established news and information services company Thomson Reuters and the 15-year-old cognitive computing innovator Digital Reasoning, recently cast a spotlight on the subject in white papers and a webcast. Participants in the latter, a Digital Reasoning event on “How to Identify and Mitigate Human Risk”, included research firm IDC Financial Insights and Point 72 Asset Management, the family-office successor to the Steven A. Cohen hedge fund S.A.C. Capital Advisors.

In Thomson Reuters Accelus’ “Tracing the True Origins of Bad Behavior: New Ways to Predict Conduct Risk Exposure”, author and behavioral risk specialist Roger Miles says that new research

coming out of academia is producing new thinking about human risk taking and predictors of bad behavior.

“We’re moving away from the rational calculus toward a more rounded understanding of why people take a risk, aside from the rational benefits,” Miles says in an interview. “They do so based on how they feel, who they are selling to, their life situation, age, employment and many other things.”

Supervisory Emphasis

More than a half decade since the global financial crisis, the intellectual framework defining behavioral risk, coupled with the high-level pronouncements on conduct risk, is influencing both regulatory supervision and the way institutions are responding.

Says Miles, “I personally find it ironic that many of the world’s businesses – the medical profession and the military, for example – have had conduct controls in place for thousands of years, and yet banking, one of the world’s oldest professions, has never had a framework for conduct control.”

He notes that in an age when face-to-face trading has been overtaken by virtualized markets, the focus of oversight has shifted more toward data and algorithms and is less about the character and trustworthiness of trading partners.

“In the old days, the fact that you were physically eyeballing the person you were contracting with” served as protection against misconduct, Miles says, adding that in a depersonalized, electronic world, new rules are needed and others need to be discarded.

Citing research by Elizabeth Sheedy of Australia’s Macquarie University on risk culture at financial institutions, and Stephen Mandis, a former investment banker now teaching at Columbia Business School and studying for a Ph.D. in sociology (see “What It Will Take to Change the Culture of Wall Street”), Miles says that firms need to abandon the assumption that published rules and codes are effective in curbing bad behavior.

From a risk management perspective, this means that firms must understand and assess both the formal organization – based on official rules and job titles – and the informal organization, or “what

actually happens" on a day-to-day basis, Miles explains. It is the latter arena that risk managers need to monitor, and that is where regulators will be looking for predictors of bad behavior.

Psychology of Risk-Taking

Research indicates that "chancers," or people who are attracted to risk, tend to be attracted to the financial sector. "Markets are a magnet for sociopaths," Miles says, and although chancers may succeed at making money, they should not necessarily be promoted to senior executive positions.

Research also shows that peer behavior is a strong determinant of what "normal" means for a given individual. "We quickly adapt to behave in ways that help us to fit in with our work group," Miles says.

"Markets are a magnet for sociopaths," says behavioral risk expert Roger Miles.

In financial firms, there are "tribal network cultures" that develop their own loyalties that defy interventions from corporate control structures, as was reportedly the case in Libor manipulations. Miles notes that such groups have their own language, social media spaces and even tacit codes of conduct. "The in-group tribe rejects any approach from the out-group or everybody else," Miles writes in his paper. The harder a regulator or risk manager might push for a behavioral change, the more likely the group will be to view this as provocation, push back or simply reject the approach.

Indeed, PwC and London Business School released a study in June on "why bankers can't be scared into doing the right thing."

So what's the solution for risk managers and the executive teams they work with?

Miles says a first step would be to understand that top-down efforts at building a healthy risk culture are doomed to failure. It turns out that for preventing bad behavior, the vaunted "tone at the top"

matters less than “tone in the middle.” He also suggests relying on independent, third-party risk consultants to conduct behavioral risk audits of the informal organization.

Beyond Conventional Compliance

Regulators will now be expecting firms to closely monitor factors that could encourage bad behavior, Miles adds.

Examples include: established companies that act as if they are invulnerable, and the related belief that regulations can’t impact them; products that are abstract and confuse consumers; a sense of territorial independence, causing firms in some instances to ignore or be casual about local laws; and overly detailed regulation that may encourage searching for, and exploitation of, loopholes.

“All of this will be harder than conventional compliance,” says Miles, adding that compliance “is no longer just about stress tests and money measurements.”

Thomson Reuters sees an opportunity, through governance, risk and compliance tools, to assist with behavioral risk management.

“We think both humans and technology have a role to play,” says Ellen Davis, a marketing director in Thomson Reuters’ Financial & Risk division. Relevant products include an online compliance training program; a customizable regulatory tracker; and an enterprise risk management platform that helps firms build out a conduct risk framework.

Intelligent Surveillance

Digital Reasoning, a Tennessee-based company that started out serving the intelligence community and began focusing on predictive analytics for the financial industry about three years ago – its venture capital funders include Goldman Sachs Group and Credit Suisse NEXT Investors – had three presenters in its June 11 webcast: Michael Versace, global research director at IDC Financial insights; Vincent Tortorella, chief compliance officer and surveillance officer at Point 72; and Jacob Frenkel of the law firm Shulman Rogers, who is a former senior counsel in the Securities and Exchange Commission’s Division of Enforcement.

Cognitive computing "needs to be an integral part of risk systems," says IDC Financial Insights' Michael Versace.

Moderator Dave Curran set the stage by saying that human risk and insider threats are now top concerns for financial organizations. Whether talking about foreign exchange or Libor rigging or JPMorgan Chase & Co.'s London Whale, they all "boil down to issues with electronic communications, email chat and whether or not communications were used to coordinate and conceal things," Curran said.

Versace pointed out that financial firms are investing almost $100 billion annually in technologies and talent for risk management and compliance. With regulators focusing more than ever on conduct risk, 30% of compliance functions will be directed at employing new technology and metrics to minimize conduct failures.

Cognitive computing, Versace says, can be a major assist in this effort, and Digital Reasoning sponsored the June IDC Technology Spotlight report, "Human Conduct Risk: Opportunities for Cognitive Thinking".

Attorney Frenkel said that in times past, one could have a discussion with an auditor about what constitutes acceptable practices. But in the age of "regulatory enforcement delight," regulators are less inclined to engage in a dialogue. They are embracing whistleblowers, and this creates a more challenging environment. "You are on your own," he said, aside from your legal assistance.

Combination of Solutions

According to compliance officer Tortorella, the solution for firms like Point 72 is to use a range of technologies to try to better understand the sentiment, tone and context of the vast number of communications being monitored and checked for compliance issues, on a daily basis. "You need different technologies to limit the number of false positives," he said.

“Our job is to find needles in haystacks and to limit the number of haystacks we have to go through,” he explained, adding, “Just monitoring keywords doesn’t work. You have to be creative and thoughtful as to how you attack communications challenges.”

Point 72 employs Digital Reasoning’s cognitive computing software, relying on its natural language processing capability to flag emails and extract notable content without human intervention. It combines this tool with a system from Palantir Technologies to judge emotional states that are expressed in writing. With such advanced analytical tools, Tortorella says, “you’re essentially narrowing the filter of things that people have to look at to the things that are important.”

He stresses that it’s absolutely critical to employ people who know how to use such technology to its best advantage. Point 72 has staff with CIA, FBI and Department of Homeland Security backgrounds, and therefore experienced with intelligence-gathering and pattern recognition.

IDC’s Versace says he views cognitive computing and analytics as “the center of the bull’s-eye” in terms of helping to better monitor electronic communications.

“It can understand phrasing and better reveal intent, rather than just focusing on words from the lexicon,” he explains. “They can predict behavior, allowing you to get ahead of whistleblower activity.”

According to IDC research, the risk investments that are paying off are analytics-based. Therefore, Versace says, it is important for risk managers to identify and align themselves with the power of cognitive computing. “It needs to be an integral part of risk systems today.”

Katherine Heires (mediakat@earthlink.net) is a freelance journalist and founder of MediaKat llc.