Fighting Fraud with Sociology

Sampson, Steven

Published in:
Impact on Integrity

2014

IMPACT ON INTEGRITY

FIGHTING FRAUD WITH SOCIOLOGY

by Steve Sampson

The Shawshank Redemption (1994), starring Tim Robbins and Morgan Freeman, is your ultimate fraud movie. In the film, an unjustly imprisoned accountant takes revenge on a brutal prison warden who has been defrauding the state by renting out prison labour to road contractors. The film has several of the familiar elements in the 'fraud triangle' (needs/rationalisations/opportunities). The elements of the triangle come together and the good fraudster ends up exposing the bad fraudster.

The fraud in this film worked because of human connections. Today, we see many fraud deterrence and detection schemes that focus on developing the most effective 'system' for parsing and classifying numbers and texts so that the suspicious data is flagged. But behind such 'analytics' there is something else: people. It is people, real people, who commit fraud. People, unlike systems, have intentions, strategies, skills, networks, values and routines.

Fraud, to put it simply, is not about money. It's about human beings. This insight is hardly new, but in our rush to develop the most efficient fraud detection system, it is often forgotten.

Fraud prevention is about deterring people from crossing a legal or ethical line. It's about preventing them from making what for us is an undesirable choice. So who is it that crosses this line? And what is it that holds them back? Is it all just about strong and weak souls? Are we dealing with the hapless fraudster unable to withstand temptation or the ruthless predator who will stop at nothing until caught? Is the human practice called 'fraud' purely a result of weak incentives for doing good and lack of effective controls on doing bad? Thinking about 'super-fraudsters' like Bernie Madoff, perusing the fraud stories, we are led to ask, 'Why aren't there more Bernie Madoffs?'.

Perhaps instead of asking why people commit fraud, we should be asking: 'What is it that keeps them in line?'. Is it because of strong ethical values in the firm? Is it fear of sanctions and controls? Or do they stay honest because they want the approval and support of their colleagues? Each of these explanations entails quite different assumptions about human nature. Some of these questions are raised when we apply the 'fraud triangle' approach, with its tripartite model of needs, rationalisations and opportunities, or the more trendy 'fraud diamond' or 'fraud pentagon' models. But these three 'causal factors' are all rather vague. They are themselves the result of other factors. Take the concept of 'need'. We all have financial needs. Why are such needs fulfilled by committing fraud? We all rationalise our actions.

(continued overleaf)

IMPACT ON INTEGRITY

What makes a fraudster's rationalisations different? We all have had opportunities for fraud. Why do some of us 'go for it'? The fraud triangles, diamonds and pentagons don't help us here.

Perhaps it is more useful to look at these questions not simply as fraud issues. In fact, such questions go to the heart of what makes people tick. Social scientists and philosophers have been dealing with what makes people tick for centuries. The general question might be rephrased as: 'Why do people accept limits to their actions, and how do they test or breach these limits?'.

Fraud specialists are not supposed to be social scientists or philosophers. They are supposed to discover, deter and prevent fraud. Not surprisingly, much of the expertise in fraud is spent on developing fraud detection systems. These systems are mostly like burglar alarms: if someone crosses an electronic or financial threshold, if some amount or item is missing from the equation, an alarm rings in the form of a red flag on a computer screen. All of us employees are now forced to leave paper and electronic trails so that others can follow our actions, in case of any weak links. If it happens, the red flag pops up. Fraud detection is like video surveillance. When nothing happens, when there is no burglar, we are happy; but when someone enters, we can observe and identify the culprit; the system works. Such detection systems may be effective in telling us when the burglar has entered the house, i.e., when someone has crossed the fraud threshold. But they tell us nothing about who the burglar is, how he chose our house, or what he expects to steal once he gets in.

Some burglar alarms take on a personal touch. They try to 'communicate' with the potential burglar by deterring entry. Hence, the warning signs, false barking dog sounds, or light sensors letting you know that you are being watched. The expectation here is that the rational burglar will minimise risk and choose another home to target. On a computer, there are the flashing entries when we enter some incorrect data, exaggerated numbers or wrong passcode. The system asks us to 'identify yourself' or 'explain this amount'.

Regardless of whether we have a more impersonal or more personalised system, all studies show that internal audits and monitoring do little to actually detect fraud. Most fraud is a continuing pattern of behaviour, the average being 18 months. More important, over half of all fraudsters are discovered not by internal audit systems but by whistleblowers and tips. So perhaps we need a more sociologically founded understanding of fraud. Here we can start with our understanding of the 'who'.

Who is the fraudster?

The bad apple. In most fraud detection systems, the fraudster is perceived as an individual who recognises opportunities – sees an open window so to speak—and due to pressing need or more acquisitive motives, will enter and take what they can. The fraud actor – be it the store accountant or a financial manipulator like Bernie Madoff—is seen as having some kind of psychological weakness. Explaining fraud comes down to describing weak individuals, with narcissistic or predator personalities. If this is true, then fraud detection must start with the HR division: filter out the undesirable psychological type before they get into the organisation. Fighting fraud means culling such types so they don't get anywhere near the accounting system.

The opportunity taker. There is an alternative approach that sees fraud as simply a set of opportunities. It is like picking up a wallet on the street. In this approach, we are all potential fraud actors: hold out some chocolate, put it in our faces, make it easy to rip off the company or to enter false data, and we will be tempted to do it. This approach operates with an idea of human nature that we are all susceptible. Fraud is a 'trap' we fall into. A 'situation'. The

IMPACT ON INTEGRITY

approach assumes that some of us are like children, that we just can't resist. Fighting fraud here means to reduce the set of opportunities so we don't give in to our base impulses. If there was no chocolate out there, no wallet lying in the street, no complicated accounting system that we could manipulate with impunity, then we wouldn't do it. If there were no fraud 'situation', there would be no fraud.

Fraud as a social act. Finally, there is a view of fraud that sees it not as a failure of character or a temptation, but as a cooperative act. In this sense, fraud is 'social', insofar as many people are involved. In this sense, defrauding a company, deceiving clients, skimming assets and falsifying receipts are all acts that take place within a human network. The fraudster may be pressured by a boss or family members to get results, he may be trying to help others by borrowing from the company, he may be part of a larger scheme, he may be part of a group or clan whose values sanction ripping off the firm or the government as long as you don't hurt us. And the fraudster may have clients or partners (third party suppliers) who themselves want to get rich quick. Madoff himself described how easy it was to get clients on board by appealing to their base instincts. He was a salesman. In this sociological view, the fraudster is part of chain of helpers, enablers, assistants, dupes, with people who push, applaud, encourage, cajole or receive indirect benefits. Fraud detection, and especially text-based fraud analytics, tries to identify such kinds of networks. Who contacted who about what? More difficult, however, is trying to understand the culture that creates and maintains these networks. This is a sociological task more than a management task. Fraud prevention means that we try to prevent such networks from forming. The problem, however, is that it is precisely informal networks of trust and cooperation which also make companies run well. Fraud is the dark side of trust.

If fraud is a social project, what should we be looking for? The obvious answer is some kind of conflict between the formally expressed values and practices of the organisation (its proclaimed 'culture') and the everyday practices of its members (their 'culture'). The simple question here is 'Where do my loyalties lie?'. 'Loyalties' is just another word for 'trust'. Whom do I trust, who trusts me? A typical question that people ask themselves is 'Do I have more loyalties to my family or to my workplace?'. We ask ourselves this question when our child is sick and we need to stay home from work. It's the same with a fraud situation. Fraud is the result of how these loyalties are prioritised (hence, even Madoff was good to his family).

Such loyalty conflicts become more acute in cases where an organisation is complex, global, and where the employees vary in skills, work situations and backgrounds. Take an international foreign aid organisation, for instance. A small group of expatriate staff is sent out from headquarters in Geneva to the office in Nairobi. Their mission is to provide help: they have personal values of 'doing good'. They have values, obligations and career paths that tie them to the home office in Geneva, but also to a global, cosmopolitan career of, say two years in Nairobi, then a year in Dakar, then to London, then back to Geneva. Diplomatic services, military commands and most global companies are based on such staff rotations: they move their people around partly in order to consolidate these company and cosmopolitan loyalties. Such rotation also serves to prevent the formation of competing, local loyalties. In humanitarian aid fraud, most of the problems come from those who have developed intimate local knowledge. Their local anchoring or support enables them to have dealings with local contractors. This local knowledge can be effective. But it is also 'the weak link'. The problem is to figure out what makes it weak in the first place? Is local knowledge all that bad?

(continued overleaf)

Impact Thought Leadership | November 2014

IMPACT ON INTEGRITY

Fraud does not simply occur at the edges or bottom of the organisation. We can find fraud networks among long-standing career employees. These people have developed deep-going social links with others and an intimate knowledge of the firm's financial or procurement system. They know what organisational procedures tend to be overlooked. The fraud is always in the details. In The Shawshank Redemption, this is how the savvy accountant prisoner defrauded the prison warden. It took him ten years, but he did it.

> What is the moral of this story? Fraud is not about money, not about systems, and not about technique. Fraud is about people.

People deceiving using their resources and strategies to deceive other people. To understand fraud, we have to know more about people, about what makes them tick. We have to get away from the idea that the fraudster is a particular type of person or that a particular situation will automatically push us into fraud. Instead, we need to look at fraud as a social process where groups and networks of people are involved; people who trust each other, manipulate each other, and who may also betray each other if the circumstances are right. After all, how many informants are themselves former criminals? These are tough questions. The answers are not readily at hand. But in social science, we learn that our work is all about asking the right questions rather than getting some kind of answer.

What about fraud deterrence and prevention? Fraud deterrence is usually a combination of the right 'policies and procedures', risk assessments, staff training and monitoring. These approaches need to be supplemented, however. Fraud prevention needs to start with an analysis of the firm's social coherence, the trust factor, and with the everyday human practices, its culture. How do we get people to feel loyalty to the firm? How do we stimulate trust? How do we avoid making everyone feel that they are under suspicion? Who trusts who with what? How do we get people to care about the minor details of organisational life in the same way they care about the minor details of their family life? It is surely the inattention to details that leads to successful frauds.

With the major changes in business and the complexity of organisational life, these questions pose a challenge. But in a simple way, they point to solutions: The best 'system' to prevent fraud will be the engagement of employees in the firm; it is the engaged people who see things that no analytics programme can identify. The engaged people will utilise the oldest analytics programme we have - intuition and judgement 1.0 - to discover that something (or someone) just isn't right. These people must have the environment which enables them and encourages them to speak up about fraud: to their own colleagues and to management. Not after 18 or 24 months of fraud, but as soon as they see it.

Developing this kind of environment requires coherence among people, what we call 'trust'. Building trust is difficult when employees are dispersed in ever-changing units, divisions or countries. But with more trust, employees will be able to see the red flags faster than the most professional fraud examiner armed with analytics software. Understanding networks, cultivating trust and allowing the exercise of judgement are better 'tools' than the most sophisticated of analytics programmes.

Steven Sampson, this month's guest writer, is an anthropologist researching anti-corruption and the compliance industry.

info@impactonintegrity.com
ES +34 917 668 044
UK +44 7787 209 200
www.impactonintegrity.com
@impactintegrity