www.informaprofessional.com/fi

Fraud Intelligence

For the prevention, detection and control of fraud in all its guises

Reputation – the greatest casualty

It has long been recognised that incidents of fraud, when they become known, impact the reputations of individuals and organisations involved, writes ***Richard Minogue****. Reputation, the perception held by others, will fluctuate in value in response to individual or corporate behaviour; it exhibits a direct correlation with expectations of performance. A good reputation is earned by consistently delivering against expectations, a bad one, the price of failing to meet them. A fraud incident is likely to contribute to a negative perception or, at the least, tarnish a positive image. We will look at the link between fraud and reputation in the organisational context and how it should be managed.*

The value of reputation

Damage implies a loss of value, but what is it that makes reputation valuable in the first place? The value of the perception held by others is a function of who these "others" are and how they will influence the organisation's ability to achieve its goals. Relevant others are often referred to as stakeholders. The organisation's reputation among its stakeholders will influence how they act, how they support, oppose or remain ambivalent to its interests.

While a discussion of stakeholder theory is beyond the scope of this article, we can give a few examples. The actual or potential shareholders of a stock company are stakeholders. If they have a positive view of company and its ability to pay dividends, they will be motivated to buy and hold shares, support the share price and the company's ability to finance itself. Current and potential customers are stakeholders, and their perceptions will influence their willingness to buy products and services. Employees and employment candidates are stakeholders, and their feelings about the organisation will affect their willingness to accept employment, remain as employees, and perform their duties loyally. Suppliers, regulatory authorities, trade unions are all stakeholders and their perceptions will affect their interaction with the organisation. A common concern among stakeholders might be formulated as: "Can I trust this organisation, to make a good product, report its results accurately, to provide job security?" Investors will not want to invest if they cannot trust the accuracy and fairness of financial reporting. Customers will not buy a product if they don't trust the company to deliver products that work, are safe, and so forth.

Clearly, the different stakeholder groups have different interests and concerns, and the individuals within each group may have very different opinions, determined by their own particular viewpoints. Beauty is in the eye of the beholder. So a reputation is really the aggregation of many individual perceptions. But it is probably safe to say that most stakeholders will see an incident of fraud as something negative and, whatever their starting point, lower their confidence in the organisation and their willingness to trust that it will deliver on its promises. The loss of trust is likely to be greatest when management is thought to have acted incompetently or inappropriately, either in failing to prevent the fraud or in failing to address it. Worse still, if management appears to condone or be involved in the fraud, stakeholder trust will be severely damaged. There may also, of course, be legal consequences.

Composite impact

As reputation is based on individual perceptions, stakeholders may differ in their responses to the same incident. Their views are likely to be coloured by factors like who is affected by the fraud? How have victims been damaged? How well did management handle the situation? Should management have prevented the fraud from occurring in the first place?

The principal victims of a financial reporting scandal, for example, would be investors who purchased or held shares based on a false understanding of the company´s value. Reporting fraud will certainly reduce investors' trust in management. Potential customers, on the other hand, if they are not also investors, might be unconcerned about financial

reporting fraud. These same customers might however react strongly to a report of fraudulent advertising by the company. Stakeholders, in other words, will view an organisation through the filter of their own particular interests.

Perpetrator, victim or target?

We also need to consider the organisation's role in the events and the nature of the incident. If the fraud was committed by the organisation or on its behalf, however misguided the motive, then the organisation finds itself in the role of *perpetrator*. If the fraud was committed against the organisation, to steal its assets for example, the organisation is the *victim*. Or the organisation may be the *target of the deception*, but not the victim. For example, in the case where the organisation's customer credit card information is stolen from a company database, the organisation is the target of deception while the victims are the credit card owners (or their banks). We need to look at each case separately.

The organisation as perpetrator

When fraud is committed by the organisation, or by its managers, the victims are likely to be stakeholders, and their trust will be directly affected. As mentioned above, investors will be affected by a financial reporting fraud; they are its victims. Perhaps they purchased shares at an inflated price or simply held their shares in the expectation that financial reports were reliable. Reputation loss among actual and potential investors is the natural and reasonable consequence. Criminal charges and shareholder lawsuits could also be a consequence, further affecting reputation by keeping the issue in the news. The reputational damage with other stakeholders, who are not investors, major creditors or regulators, would probably be less severe.

In a fraud that involves systematic overcharging for products sold, the primary victims are customers who were overcharged, and the reputational damage within this group will be greatest. Secondary reputational effects on investor-stakeholders may arise when the customer dissatisfaction leads to loss of sales and market share.

A third example might involve organisations who violate environmental, anti-corruption and human rights obligations. Such action might not constitute fraud, in the strict legal meaning, but is similar both in execution and consequence. The shipping company that secretly dumps waste into the ocean in order to avoid paying for legal disposal is performing a deceptive practice in order to save money. Incidents of this kind, where the victims are the general public, are likely to damage reputation across a broad range of stakeholder groups.

We need to consider one very special group of stakeholders – the employees. These insiders who have extensive daily contact with the organisation and who also depend on the organisation for their livelihoods, are extremely sensitive to misdeeds by their employer, regardless of who the victims might be. The importance of the organisation's internal culture is widely recognised as a critical factor in managing the risk of fraud, and managing all kinds of risks. Clearly, the organisation's reputation among its own employees is a major component of internal culture.

The organisation as victim

If the organisation itself is the victim of fraud, reputational damage can occur if affected stakeholders conclude that management was negligent or incompetent in failing to prevent the incident from occurring in the first place. Reputation among investors is the most obvious casualty, as they see the value of their investment declining due to perceived incompetence. The extent of the damage will be proportional to the size of the fraud. Small or medium-sized frauds may not have much effect at all.

However, we should again consider the effect on the employee-stakeholder group, and the internal reputation of the organisation. Employees will be very interested and concerned. Their job satisfaction and job security are directly related to management competence. Even relatively small fraud incidents that do not directly affect the bottom line can erode employee confidence in and respect for management.

Some employees may also be tempted by what they see as an opportunity to arrange extra advantages for themselves!

The organisation as target

Organisations often have custody of privileged, more or less confidential information that belongs to their customers. This might include, for example, credit card details, email addresses, or even medical records. Criminals frequently target organisations to obtain confidential information for fraudulent exploitation.

In these cases, the organisation has neither suffered a direct loss as a victim nor attempted a fraudulent gain as the perpetrator of the fraud. The main effect on the organisation will be the resulting loss of reputation among the victims, who will no longer be willing to trust the organisation with their sensitive information. Once again, perceived management negligence or incompetence is the problem. If it happened once, it can happen again.

Thus, the reputational damage ensures that the organisation will also be a victim.

Is fraud inevitable?

The obvious solution for protecting reputation would seem to be to avoid all fraud incidents through competent management and adequate internal control. Unfortunately, fraud is inherently difficult to prevent. In any organisation, a substantial amount of trust is absolutely necessary, both internally and in respect of outside parties. We trust managers, employees and suppliers to deliver. We trust customers to pay for goods and services they receive and we trust government institutions and their employees to perform their duties without corruption. Absolute central control is not practicable; we have no choice but to delegate. Where there is trust, there is always the possibility of betrayal, the possibility of fraud and corruption.

There is an expectation gap here that needs to be addressed. While, in practice, a certain amount of fraud is inevitable, the expectation among many stakeholders is that management should be able to prevent all fraud. When fraud inevitably occurs it will often be seen by stakeholders as evidence of management weakness. This remains true whether the organisation is in the role of perpetrator, victim or target. Managers themselves may share this perception and tend to be ashamed even if they were not at fault. Their instinctive reaction when faced with a suspected fraud situation is to look for a resolution that avoids attention, avoids exposing their perceived weakness or damaging their personal reputation or that of the organisation. Since investigating and exposing the fraudster will create unwanted publicity, managers often prefer to make a deal that allows the fraudster to escape punishment and the organisation to escape attention.

Ironically, the cover-up is stronger proof of management weakness than their failure to prevent an incident. If and when the fraud incident and cover-up find their way to the public attention, the reputational damage will be greater than the incident itself would have caused with no cover-up. And rightly so! But even if the cover-up is successful as regards external stakeholders and the public eye, it will not fool employees or prevent damage to the internal reputation. On the contrary, employees see the cover-up as proof that internal fraudsters will not be punished; perhaps they will even be rewarded with new positions or generous termination payments. The organisation develops an internal reputation that reduces employee respect and increases the likelihood of new incidents.

Enhancing reputation through Fraud Risk Management

In a system based on trust, we must accept the possibility that trust will sometimes be betrayed. We must therefore understand and accept that management cannot be expected to prevent all fraud. It follows that if a fraud occurs it is *not necessarily* a sign of management weakness or failure. Rather, if a fraud event is detected at an early stage and properly addressed, we should interpret this as evidence of management strength.

An effective Fraud Risk Management plan might include the following:

1. Raise employee awareness and develop an internal culture that is resistant to fraud;
2. Train managers, ensure they have realistic expectations regarding fraud risk;
3. Continuously identify and evaluate specific fraud risks;
4. Implement reasonable preventive and detective internal controls;
5. Avoid inadvertent creation of fraud incentives;
6. Proactively search for any signs that controls are being circumvented;
7. Ensure channels of communication facilitate reporting of concerns;
8. Be prepared – develop a fraud response plan and educate managers;
9. When fraud is suspected, manage it, do not cover up.

Investigation is not necessarily the best approach in every case of suspected fraud. Incidents detected in their early stages may often be expeditiously resolved by other means. However, in more serious cases, when fraudulent activities have sunk their roots more deeply, management has a responsibility to themselves to dig deeply in order to ensure that the causes are addressed.

While fraud may be inevitable its pervasiveness can be reduced through the deliberate development of an internal culture based on mutual respect and ethical behaviour. This requires an enlightened and proactive approach to fraud management as opposed to a complacent and reactive approach. Fraud management should be dedicated to controlling the matches not fighting the fire; it is about reducing the opportunity, avoiding the inadvertent

creation of fraud incentives, and raising internal awareness. This requires enlightened governance encompassing sound leadership and professional management.

The importance of communication

A good reputation with investors, customers, suppliers, employees and other stakeholders is a valuable asset. While reputation is intangible, it cannot be without substance. A good reputation must be earned through strong and ethical management practice. Top management and the Board must set the ethical guidelines, dedicate resources and demonstrate their conviction through the example of their own behaviour.

Strong management includes the ability and willingness to address fraud incidents and other negative events, and communicate them promptly and honestly, internally and externally.

In the case where the organisation becomes the perpetrator of fraud, reputational damage can be reduced by truthfully demonstrating that the incident is the result of the misguided actions of a few, that it is unacceptable to the organisation and against its clear policy. The focus cannot simply be to find scapegoats; the organisation needs also to admit its failure to prevent the incident and its determination to prevent any repeat. Management also needs to take every action to mitigate the consequences for the victims.

If the organisation is itself the victim of fraud, internal and external communications tend to be complicated by legal considerations. But the message must still be that the organisation does not tolerate or reward fraud.

Through truthful and proactive communication, and a willingness to treat any incident as an opportunity to improve, the organisation can gain the sympathy and understanding of its stakeholders and contain reputational damage.

Richard Minogue *(richard.minogue@septiagroup.com) has over 35 years' experience in general management, financial management, internal audit, fraud investigation and integrity risk management. He has conducted assignments on all six continents and regularly lectures and conducts training in integrity risk management. Richard is co-author of "The Anatomy of Fraud and Corruption" (Brytting Minogue and Morino, Gower 2011).*