Fraud, Directors and the Board

*Prof. Colin Coulson-Thomas

As well as building and governing companies, directors and boards should also seek to protect them from malevolent intentions. Many companies are under attack 24/7 from hackers and fraudsters. Some criminals aim to steal money or information that can be monetised. Others look for ways of laundering the proceeds of crime. Some use tried and tested methods that often succeed. Others push the boundaries. Old scams reappear in new guises. Criminals can be inventive and innovative.

Directors and boards cannot afford to be naïve in the face of multiple threats. Not all of them may be external. People within a company might attempt to profit by sharing insider information with associates and friends. Criminal activity can include price fixing and collusion in the setting of interest rates. Directors should not assume that existing anti-fraud and risk management practices are effective. Unauthorised activities can implicate a company in charges of fraudulent conduct.

Exposure to the risk of fraud is a consequence of contemporary operation. It is ever present in many situations, contexts and locations. It is also being perpetrated on an industrial basis, as criminals and others take advantage of technological and other developments. For example, the internet of things and larger numbers of connected devices create new opportunities for criminals. Innovation and entrepreneurship can increase risks for the unwary, particularly during transition and change.

The Counter-fraud Challenge

Fraud is a form of theft by lying. It is also a crime that is significantly under reported. Many who suffer losses feel ashamed and embarrassed. They hide that they are victims. If they believe the prospect of recovering stolen money is low, they may quietly take a hit. Criminals often feed on large numbers of small strikes. The losses suffered by many people can add up to a large amount. In some countries, the majority of businesses have suffered effective malware attacks of some form.

A higher proportion of small businesses may be victims of malware and other cyber attacks. The cost of preventative and protective measures can represent a bigger proportionate burden for a smaller enterprise. They may lack the critical mass of qualified staff needed for greater resistance and resilience. In an arms race between criminals and their targets, many companies do not have the resources, discipline or focus to win. Cherished openness and informality can increase vulnerability.

Governance structures and corporate practices tend to follow a pattern. They are often rule and logic based, and designed to cope with defined categories and particular situations. To a fraudster or hacker they may be predictable. To reduce cost and variation, corporate processes and systems often rely upon classification, standardisation and automation. People operating them may be given little discretion to respond to the particular requirements of individual callers or customers.

Criminals can be more flexible. While corporate staff are busy, distracted and under pressure to complete all transactions, fraudsters can plot and scheme. They can try different options. They can modify their approaches to exploit loopholes or home onto a perceived vulnerability. If they smell blood they can persist. They just need to succeed at enough attempted frauds to deliver an acceptable return on their efforts. Like gamblers, they operate in a world of probabilities. To combat them one needs to understand their motivations and how criminal minds operate.

Recognising Patterns of Fraud.

Although new approaches to enticing desired responses and overcoming defences are continually being tried, some attempts at fraud follow certain patterns. For example, different phishing attacks may have features in common. Making people aware of these might alert them to suspect emails. Many fraudsters can cover their costs if a very small proportion of recipients click upon an attachment, or respond with password information.

Cyber criminals are becoming more focused and determined. They devote more effort to learning about a target business prior to launching a planned attack to steal larger amounts of money or data. Once entry is secured via a business email account, some time may be spent “casing the joint”. Criminal possibilities are assessed without alerting a potential victim. Stolen data, code and entry and other tools can all be purchased and exchanged on dark forums. Many criminals have built well equipped operations that are either as sophisticated as those of most of their targets, or more so. As cyber and other threats mutate, obtaining and developing the skills required to operate adequate defences is not easy. There is also a risk that some of those who are trained might themselves decide to become hackers. Defences may need to be continually changed and updated if they are to remain secure. When doing this, many companies play catch up in response to new forms of attack.

Companies should continually scan for threats and monitor trends and developments in the threat landscape, in order to quickly distinguish between problems they feel can be dealt with internally, and those which will require external assistance and/or collaboration if they are to be addressed or guarded against. Criteria may need to be set for determining which risks or intrusions would warrant disclosure and collaboration with law enforcement agencies.

Cost-effectiveness Considerations

Insurance to cover certain forms of fraud may be difficult to obtain at an affordable price. The cost of preventative measures can be compared with those of incidents of fraud and the likelihood of their

occurrence. More sophisticated criminals also monitor the cost-effectiveness of their operations. Like entrepreneurs, they think in terms of probabilities, risks and returns.

Measures and responses that increase the risks faced by criminals, lower their returns, reduce the probability of a successful strike and raise the prospects of being tracked, caught and/or closed down may cause them to pause. They might give up, if continuing does not seem worthwhile. Effective individual and collective action by companies, regulators and other agencies can deter attacks and cause criminals to switch their attention to softer targets.

Counter-fraud activities and agencies may also have to cover costs and show value for money. In judging performance, should one add the cost of preventative and counter measures, and disruption caused, to any financial losses suffered? Awareness of incidents of fraud can lead to a loss of trust. Opportunities that are missed as a result can be difficult to assess. Many companies do not report fraud, fearing this might reduce prospect, customer and investor confidence.

Sharing information about attacks and how best to address them can be very beneficial for tackling certain forms of fraud, especially cyber crimes. Directors may be concerned to protect intellectual property and commercially sensitive information during the process. However, these may be more at risk if reluctance to cooperate results in insufficient information to assess what is happening across a market or sector. This can complicate prioritisation and the planning of responses.

Companies are often less worried about small financial losses than they would be about a major leak of personal or corporate data. However, the lack of vigilance on the part of some people that causes them could reveal a systemic weakness. This might be exploited by other criminals intent upon making a smaller number of much larger gains. The possible consequences of all breaches and deficiencies should be carefully considered. Small tremors can be harbingers of major quakes.

Assessing Corporate Exposure

Directors should be alert to where a company and its people are vulnerable. Often the easiest way into an organisation's systems and data is via a naïve or slack employee, or a connected party who leaves a door open or inadvertently admits a criminal to a corporate network. After entering by a back door the criminal can move to where “valuables are stored”. The full range of communications are at risk. Large numbers of people become victims of email, text, postal and telephone scams.

A scam occurs when a victim authorises payment, which may not be the case with fraud. Like fraud, a scam is criminal behaviour. Persistent scam callers set out to build trust. A proportion of those targeted reveal their passwords. Anti-fraud newsletters and other communications can alert people to the consequences of becoming a victim and the risks of compromising the security of corporate systems. Basic guidance should not be overlooked. Many people put images and details of their activities, movements, homes and offices on social media. Such disclosure gives criminals a mass of information, including notice of when they are away.

People should be vigilant in relation to their own actions and what is going on around them. They should look out for signs of concealment, defensive behaviour and lying, and where such behaviour might succeed. When in doubt or concerned, they should alert a corporate and network security team. Confidential reporting links and help lines may be welcomed and used by those with concerns. Whistleblowing policies can enable more cases of fraud to be identified, but people may require reassurance that they will not suffer adverse consequences if they speak up.

Many manufacturers could do more to prevent the misuse of products that are connected to the internet. Developers of corporate software need to be aware of security issues. In many countries, there are various sources of information and intelligence that companies can turn to, and public and other services they can access, to better protect themselves. Care should be taken to ensure that corporate policies to reduce fraud and abuse do not inhibit innovation and responsible risk taking.

Anti-fraud Strategies and Policies

Cyber security and anti-fraud strategies and policies should be higher on some boardroom agendas. Many directors need to step up to their responsibilities in relation to fraud and other criminal activity which can have immediate and lasting consequences. They are also a threat to market systems and societies within which companies operate. Directors have a duty to act in the long-term interests of those to whom they are accountable and for whom they are responsible.

Boards should balance costs and benefits and take stakeholder interests into account when taking decisions. Expensive arrangements based upon previous experience may fail to provide protection against new forms of attack. Affordable ways of adapting defences in the light of a changing risk and threat environment, flexibility, 24/7 monitoring, and responding decisively and rapidly when frauds and hacks occur are all desirable.

Checks, alerts, help and monitoring and reporting arrangements can be built into processes and support tools. It is good business sense and a moral and social responsibility to collaborate to protect a company - and its supply chain and stakeholders - and confront significant threats to future operations and sustainable development. Customers, suppliers, staff, associates, investors, business partners, public bodies and others can all become victims of fraud and other criminal activities that are increasingly undertaken across national borders and on an international basis.

Given the nature of threats, should boards leave it to law enforcement agencies with their budget and manpower constraints to act alone to stem the criminal tide? If boards do not take steps to protect companies and their stakeholders, report and share information, and collaborate with regulators, law enforcement and other agencies, Governments may become more involved. They have a duty to protect citizens. Like companies they face difficult choices. Some measures might involve extra bureaucracy, further costs and additional taxation. Actions such as greater powers to snoop or intervene when vital services are interrupted may prove unpopular with many directors.

While people are wedded to greater connectivity, internet transactions and other activities, remote access, portable technology, e-government and other on-line services, and flexible working and learning practices, our vulnerability as individuals, communities and societies may continue to increase. If our way of life, markets and the capitalist system are to survive, directors and boards must play their part in corporate and collective efforts to protect them.

***Prof. Colin Coulson-Thomas is IOD India's Director-General, for UK and Europe Operations, also holds a portfolio of board academic and international roles, and has advised directors and boards in over 40 countries.**