FRAUD, SECURITY RISKS AND CORPORATE RESPONSES*

Prof. Colin Coulson-Thomas

Prof. Colin Coulson-Thomas advises boards and has helped directors in over 40 countries to improve board and corporate performance. He leads the International Governance Initiative of the Order of St Lazarus, is Chancellor and Professorial Fellow at the School for the Creative Arts, Director-General, IOD India, UK and Europe, chair of the Risk and Audit Committee of United Learning and Honorary Professor at Aston University. Author of over 60 books and reports he has held professorial appointments in Europe, North and South America, Africa, the Middle East, India and China, and has served on many corporate boards and UK public sector boards at local and national level. Colin was educated at the London School of Economics, London Business School, UNISA and the Universities of Aston, Chicago and Southern California. He is a fellow of seven chartered bodies and obtained first place prizes in the final exams of three professions.

Directors, boards and the companies they endeavour to lead face a variety of risks. They range from natural disasters that might be infrequent and difficult to predict, to errors, mistakes and unintended consequences which may occur on a regular basis, and movements in currency rates which may be in a continual state of flux. Some risks are newer than others and older risks may now be caused in new ways. Directors should not assume that risk management is effective (Hubbard, 2009).

A degree of risk can be healthy and viewed as an indication of life in a market economy. While innovation and entrepreneurship can both be desirable they may increase risk (Brockhaus,1980). Traditionally, it has been assumed that risk and return have been related (Modigliani and Miller, 1958), but applications of performance support may enable returns to be increased and risks reduced or contained (Coulson-Thomas, 2012a & b, 2013).

One almost universal and traditional area of risk which is ever present in many situations, contexts and locations is fraud. It is now 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 have created a new frontier of opportunity for criminals. Many directors should devote more attention to fraud, cyber-fraud and other cyber crimes such as hacking.

THE COUNTER-FRAUD CHALLENGE

Fraud is a form of theft by lying. It is a crime and one that is significantly under reported. Many of those who suffer losses feel ashamed and embarrassed. People and organisations rarely want to reveal that they are victims. They may also believe that the prospect of recovering money that has been taken is low. They quietly take a hit. Much of the criminal eco-system feeds upon large numbers of small strikes. These 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.

An even higher proportion of small businesses are likely to have been 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 are also less likely to maintain the critical mass of qualified staff needed for greater resistance and resilience. In the equivalent of an arms race between criminal and potential victims, many companies do not have the resources, discipline or single minded focus to win. The openness and informality they cherish can also make them vulnerable.

Governance structures and corporate processes and systems tend to follow a pattern or blueprint. They are often rule and logic based. They are designed to cope with defined categories and particular situations. To a fraudster or hacker they may be predictable. In order to reduce cost and variation corporate systems and processes often rely upon classification, standardisation and automation. The people who operate them may be given little discretion to change responses to meet the particular requirements of individual callers or customers.

In contrast, criminals can be more flexible. While corporate staff are busy, distracted and under pressure, fraudsters can plot and scheme. They can try different options and modify their approaches to exploit loopholes or home in on what they perceive as an area of vulnerability. If they smell blood they can persist. The issue for them is not completing all transactions, but succeeding in enough of their attempted frauds to cover their operating costs. Like gamblers, they operate in a world of probabilities. To combat them one

needs to understand their motivations and perspective and their view of opportunities and vulnerabilities (Hussain, 2014).

Businesses recognise the distinction between structured activity to cope with most eventualities and occasional chance events, where insurance may be a better option than relatively high expenditure on attempts to prevent an incident with a low probability of occurrence. It may make sense to pay a regular premium and raise a claim as and when a risk materialises. However, in the case of some forms of crime such as cyber-crime, insurance may be difficult to obtain at an affordable price.

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 may alert them to those emails which might be suspect. Many fraudsters only need a very small proportion of recipients to click upon an attachment, or to respond with password information, in order to cover their costs.

Criminals who carry out cyber attacks are becoming more focused and determined. Greater effort may now be devoted to preparation and 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 in various forms of scouting. Fraudsters or hackers may aim to assess criminal possibilities without alerting a potential victim. Stolen data, code and entry and other tools and techniques can all be purchased and exchanged on dark forums. Many criminals have built up well equipped operations that are either as sophisticated as those of most of their targets, or are more so.

The nature of mutating cyber threats is such that it is difficult for many individual companies to keep their defences current and to cope without help from others (Coulson-Thomas, 2016). 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 go on to become hackers. Defences may need to be continually changed and updated if they are to remain secure. In doing this many companies may have to 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 identify and scope potential problems. A company needs to be able to quickly distinguish between problems it feels it can deal with itself 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. Encouraging people to read about a fictional corporate fraud situation could be a further way of alerting people to risks and practical counter-measures (Pickett, 2007).

COST-EFFECTIVENESS CONSIDERATIONS

More sophisticated criminals monitor the cost-effectiveness of their operations. Like entrepreneurs, they think in terms of probabilities, risks and returns. With more opportunities to monetise what is taken, returns from cyber-crimes such as data theft may be increasing (Coulson-Thomas, 2016).

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 and closed down or caught may cause them to pause. They may 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 also have to cover their costs. They may need to show value for money. In judging performance, one should add the cost and disruption caused by preventative and counter measures to any financial losses suffered. Potential opportunities that might have been missed due to a loss of trust, following awareness of one or more incidents of fraud, can be difficult to assess. Many companies do not report fraud because of concerns that knowledge of them might reduce the confidence that prospects and customers and other stakeholders have in them.

The sharing of information about different forms of attack 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 this process, but these may be more at risk as a result of a reluctance and failure to cooperate, where this results in insufficient information to assess the true nature of what is happening across a market or sector. Inadequate knowledge of a situation complicates 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, a small loss to a fraudster who operates on the basis of making lots of small strikes due to a lack of vigilance on the part of some people could reveal a systemic weakness. This might be exploited by another criminal 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.

CORPORATE EXPOSURE AND RESPONSES

Companies need to be alert to where they and their people are vulnerable. Often the easiest way into an organisation's systems and data is via a naïve and/or slack employee who leaves a door open or inadvertently admits a criminal to a corporate network. After entering by a back door the criminal can move around to the equivalent of the “front of the house where valuables are stored”. The full range of communications are at risk, as large numbers of people regularly 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, but like fraud a scam is a category of criminal behaviour.

Persistent scam callers set out to build trust. A proportion of those approached usually reveal details of their passwords. Anti-fraud newsletters and other communications can be used to 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 encouraged to be vigilant in relation to their own actions and what is going on around them. They should be on the look out for tell-tale signs that someone might be lying (Houston et al, 2013). When in doubt or concerned, they should be encouraged to alert those responsible for corporate and network security. Confidential reporting arrangements and help lines may be both welcomed and used by those with concerns. An effective whistleblowing policy can also enable more cases of fraud to be identified (ACCA, 2016), but people may need to be reassured they will not suffer adverse consequences if they speak up (Alford, 2001).

Manufacturers should consider ways of preventing the misuse of any of their 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 needs to be taken to ensure that corporate policies to reduce various risks do not inhibit innovation and responsible risk taking.

COLLABORATION AND COLLECTIVE ACTION

Directors should be wary of complacency. Being watertight yesterday does not mean one's company will survive tomorrow's attack. The digital landscape and threats within is are continually changing and evolving. An report from ACCA (2013) suggests that digital technologies and their applications are evolving more rapidly than individuals and organisations can adapt and put in place ways of protecting themselves from their misuse. Many companies are struggling to cope and more collaborative action is needed from sharing information to international action.

In some cases, the most useful actual or potential anti-fraud collaborators are equivalent organisations and/or agencies in similar situations in other countries, rather than local companies in one's home country. For example, anti-fraud agencies in cities that are major financial centres may find they have much in common in terms of the challenges they face and who they are up against. It makes sense for them and similar companies in certain sectors to cooperate whether by exchanges of staff, joint working on preventative measures or addressing particular threats.

There are many forms of cooperation which may or may not be acceptable, depending upon the terms and arrangements of each collaboration framework. The latter may specify formats in which data, insights and experiences will need to be captured, stored and transmitted if it is to be effectively shared. Paradoxically, the separation of data in terms of storage and access, and the use of different programmes and devices to limit access for hackers who breach outer defences, can make data, information and knowledge more difficult to assemble and share. Collective and international action through trade associations and other sectoral bodies can also be helpful.

As well as yielding benefits, collaboration can involve risk. Apart from the risk of a sharing network itself being compromised, there is the possibility of becoming swamped and distracted by an excess of information, some of which might not be relevant to the problems faced by a receiving company. Also, law enforcement agencies do not have unlimited resources. They cannot follow every possible lead. Hence the need for selectivity and focus. Areas to concentrate upon are where there are known vulnerabilities, the consequences of penetration and theft could be serious, and recovery and/or compensation costs would be high.

COMPANIES AS OBSTACLES

Some directors put too much faith in corporate defences. They may feel that a company can cope on its own. The risk of fraud, hacking and failure is sometimes greatest when senior people are at their most confident and others defer to them and go along for the ride on account of their apparent and past success. Hubris can lead to unfortunate and serious consequences (Nixon, 2016).

From the perspective of law enforcement agencies companies can sometimes be obstacles rather than allies in their attempts to track down and catch criminals. For example, when companies take steps to protect their customers' communications and devices from state surveillance agencies this can create new opportunities for criminals. Law enforcement agencies may no longer be able to monitor the planned and ongoing activities of suspects and accumulate the evidence that would bring them to justice. Certain devices cannot be opened even when court orders have been obtained.

Most directors will instinctively want to protect a company's customers. Many of them might wish to shield customers and users from a snooping Government. Hence the use of shields, encryption and the design of products such as mobile communications devices with high levels of security for informed users. Directors may have to balance the desire of their customers for privacy, encryption and secure devices against the risk that a proportion of users may be using their company's public networks and devices for criminal purposes to the detriment of other customers they seek to protect.

Vocal lobbies put the case for freedom from surveillance. They stress the risk that giving greater powers to state authorities could lead to their abuse. Certain adoptions of technological developments, such as the greater use of Blockchain applications which record each step in a process, could create audit trails that might allow liability to be established, for example in relation to a claim of mis-selling. The same sort of evidence could help to bring external parties to justice.

Certain Governments sponsor illegal attempts to secure intellectual property and other valuable information. Some companies that are sensitive to external surveillance by state authorities may themselves use various espionage techniques, such as eavesdropping on their commercial rivals. They may seek advice on how to obtain information about their competitors on a systematic basis (Carleson, 2013). Companies in sectors such as defence and aerospace may be particularly at risk. They should take steps to help their staff resist attempts by others to obtain information from them.

As already mentioned, the internet of things is creating new areas of vulnerability that need addressing. Many customers do not change the default passwords used by manufacturers and suppliers, thus allowing unauthorised access to connected products and devices. External control of ones fridge might be inconvenient, but unauthorised control of ones car could be life threatening. New and potentially expensive areas of corporate liability could be established.

PROBABILITY AND PRIORITISATION

When and where collaboration occurs, and access to data and communications is obtained by state authorities, there may be other bridges to cross. Although large numbers of frauds may be regularly

happening, these can represent a small proportion of an enormous volume of financial transactions that are occurring on a daily basis. Given the inconvenience that can be caused by blocking transactions, not to mention the protests and damages claims that could result, fraud monitoring activity has to focus upon a small minority of them that appear unusual and/or suspect. It has to do this in a way that does not impose disproportionate cost and inconvenience upon the great majority of users of various services.

The volume of transactions that is occurring, and the number of messages being sent, are such that without intelligent filtering and monitoring, both preventative systems and people may be swamped. Search criteria need to be established, according to the prioritisation of risks, the availability of technical solutions and whether or not particular targets or threats have been identified. For most companies, a high priority should be put upon protecting customers. Extra vigilance may be required when major and IT projects are involved (Flyvbjerg, 2003, Flyvbjerg and Budzier, 2011).

Some threats with particularly low probabilities of occurrence can have the largest impacts if and when they succeed. An example would be a planned terrorist attack designed to inflict the maximum of damage and disruption. Simultaneous action against a number of leading banks could be designed to bring down a banking and financial system. The consequences could be severe and widely felt. They could include a break down of law and order. Many companies could only operate for a limited time without access to credit and/or an inflow of cash, while unrest might occur quickly among unpaid citizens.

NEW AREAS OF CONTROL

Governments, companies and other organisations need to be alert to new areas in which controls might be required. Some of these may be in traditional arenas. Law enforcement agencies could seek additional powers to access private data and track suspects, while companies might, as already mentioned, resist and seek to protect their customers from unwanted intrusion and interference. Controls may be needed in fields that are opening up. For example, what if any controls and conditions should be placed upon the “things” that are connected to the internet of things? How should such connections be protected? Should they be monitored and for what purposes?

There is a risk that digital skills training could equip future hackers to cause harm. Should companies be more circumspect in terms of who receives certain forms of exposure to advanced tools and techniques? Should digital skills development be accompanied by ethical awareness training? What are the best tests and checks to use when selecting people for cyber security roles and related development activities? Should greater use be made of biometrics in identity checks, such as those for securing access to sensitive areas?

Thought needs to be given to the allocation of roles and responsibilities for dealing with fraud and other risks. Internal and external auditors have a responsibility for assessing processes and internal controls, but what about supply chain and other external networks? A chief financial officer and his or her team will have a particular interest in preventing financial fraud. Chief security, information and knowledge officers will be keen to protect corporate data, information and know-how. The HR director and team should be alert to the human factors that can result in people who have hitherto been trusted engaging in fraudulent activities (Hussain, 2014). To what extent should they and others have a remit to protect the interests of stakeholders and wider society from illicit activities?

WIDER CORPORATE RESPONSIBILITIES

The social responsibility of business has long been an issue (Bowen, 1953). Some boards have a narrow and largely internal focus when matters of security and fraud are concerned. Law enforcement agencies are involved as a last resort, as and when needed. Should boards just focus upon minimising harm to the entities for which they are responsible, or should they acknowledge wider corporate social responsibilities? For example, should they prevent future harm to fellow citizens and external parties by collaborating with other organisations and relevant agencies and authorities in the building of collective defences and the tracking down of fraudsters and hackers?

Sometimes it might appear that the easiest option is to look the other way and just focus upon one's core business, but is this always the right course of action? Data lost in seconds might result in consequences that may take individual victims of a crime such as identity fraud many days to address. In such situations, a company might have to act quickly to protect its customers. On other occasions, what is exposed to a hacker may be well backed up and of little value or danger to others if it is accessed and downloaded. In such

circumstances, a well prepared company may have options, including an opportunity to hit back.

Once an incident of hacking has been detected an instinctive reaction may be to “shut the door”. However, from a law enforcement perspective there might be merit in allowing a breach to continue long enough to enable a hacker or criminal source to be tracked. Should significant harm result from a delay in instituting counter measures, a decision not to close down quickly may well be criticised. Calculating probable costs and benefits in such circumstances may seem like sophistry, but should institutions facing large numbers of daily threats from hackers do more to collaborate in efforts to monitor, track and also respond to the major threats they face? In certain cases might there be a case for pro-active action where this is legal and appropriately authorised?

THE ROLE OF BOARDS

Corporate governance should strike the right balance between risk, compliance and performance (ACCA, 2014). Cyber security and anti-fraud strategy 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 that can have immediate and lasting consequences. They are also a threat to the market systems and societies within which companies operate. Directors have a duty to act in the long-term interests of the entities for which they are responsible.

Boards should also balance costs and benefits and take the interests of stakeholders into account in their decision making. Expensive plans and arrangements based upon previous experience may fail to provide protection against new forms of attack. To what extent should resources be devoted to addressing unknown and unpredictable events (Sagarin, 2012)? Organic evolution of 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 might be an affordable option.

Additional checks, alerts, help, monitoring and reporting arrangements can be built into processes and support tools (Coulson-Thomas, 2012a & b, 2013). It is good business sense as well as a moral and social responsibility to collaborate to protect a company - and its supply chain and stakeholders - and to confront significant threats to future operations and sustainable development. Customers, suppliers, staff, associates, investors, business partners, public bodies and others can all be victims or potential victims of fraud and other criminal activities that are increasingly undertaken across national borders and on an international basis.

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

So long as people are wedded to greater connectivity, the use of the internet for 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.

REFERENCES

ACCA (2013), *Digital Darwinism: Thriving in the face of technology change*, London, Association of Chartered Certified Accountants, October

ACCA (2014), *ACCA Best Practice Principles for Governance, Risk and Performance*, London, Association of Chartered Certified Accountants, December

ACCA (2016), *Effective speak-up arrangements for whistle-blowers: Recommendations for Director*s, London, Association of Chartered Certified Accountants, May

Alford, C. F. (2001), *Whistle-blowers: Broken Lives and Organizational Power*, New York NY, Cornell University Press

Bowen, Howard (1953), *Social Responsibilities of the Businessman*, New York, NY, Harper & Row

Brockhaus, R. H. (1980), Risk Taking Propensity of Entrepreneurs. *Academy of Management Journal*, 23, pp 3509-520

Carleson, J. C. (2013), *Work Like a Spy*, *Business Tips from a Former CIA Officer*, New York, NY, Portfolio/Penguin

Coulson-Thomas, Colin (2012a), *Talent Management 2*, *A quicker and more cost-effective route to the high performance organisation*, Peterborough, Policy Publications

Coulson-Thomas, Colin (2012b), *Transforming Public Services*, *A quicker and affordable route to the performance public organisations*, Peterborough, Policy Publications

Coulson-Thomas, Colin (2013), *Transforming Knowledge Management, A quicker and affordable route to the high performance organisation*, Peterborough, Policy Publications

Coulson-Thomas, Colin (2016), Cyber Security, Risk Governance and the Board, *Director Today*, Vol II Issue X, October, pp 7-9

Flyvbjerg, Bent (2003), *Megaprojects and Risk: An Anatomy of Ambition*, Cambridge, Cambridge University Press

Flyvbjerg, Bent and Budzier, Alexander (2011), Why Your IT Project May Be Riskier Than You Think, *Harvard Business Review*, Vol. 89 (9), pp 601–603

Hubbard, Douglas (2009), *The Failure of Risk Management: Why It's Broken and How to Fix It*, Somerset, NJ, John Wiley & Sons

Hussain, Maryam (2014), *Corporate Fraud: The Human Factor*, London, Bloomsbury

Houston, Phillip, Floyd, Michael and Carnicero, Susan with Tennant, Don (2013), *Spy the Lie: Former CIA Officers Teach You How to Detect Deception*, New York, NY, St Martin's Press

Modigliani, Franco and Miller, Merton (1958), The Cost of Capital, Corporation Finance and the Theory of Investment, *American Economic Review*, 48 (3), pp 261–297

Nixon, Matt (2016), *Pariahs: Hubris, Reputation and Organisational Crises*, Faringdon, Oxfordshire, Libri Publishing

Pickett, K. H. Spencer (2007), *Corporate Fraud: A Manager's Journey*, Chichester, John Wiley and Sons

Sagarin, Rafe (2012), *Learning from the Octopus, How secrets from nature can help us fight terrorist attacks, natural disasters, and disease*, New York, NY, Basic Books

*PUBLICATION

Published by India's Institute of Directors within an edited book of papers to accompany the Global Convention on Corporate Ethics & Risk Management held on 17th and 18th February at the Bombay Stock Exchange, Mumbai, India. The citation is:

> Coulson-Thomas, Colin (2017), Fraud, Security Risks and Corporate Responses in Ahluwalia J. S. (Editor), *Corporate Ethics & Risk Management in an uncertain world,* Mumbai, IOD Publishing, 17th February, pp 67-76 [ISBN: 978-81-930987-0-7]