Cyber Risk Management, Collaboration and Governance

*Prof. Colin Coulson-Thomas

Directors and Boards face dilemmas. We are expected to be entrepreneurial and proactive to ensure the future success of our companies. At the same time, we are expected to be prudent and to ensure compliance and maintain control. We want our people to challenge and push at boundaries, while also behaving ethically and observing the law. Is there a conflict between being entrepreneurial and maintaining prudent and necessary control? Are we getting the balance between them right? Can we simultaneosly excel at both of them when faced with cyber security and other threats?

Owners of an established and mature company whose strategy is primarily defensive and protective of an achieved position may welcome caution. They might regard risk averse directors as responsible citizens rather than wet blankets. But, what about the ambitious and entrepreneurial who want to move quickly, exploit opportunities and grow rapidly? What if we realise that more than incremental improvement is required to cope with challenges and seize opportunities?

What if we need to be much more flexible in the face of constantly mutating cyber security challenges? What if we need to be more creative and innovative to exploit disruptive technologies and go out in front and explore and pioneer? Have some directors and boards - and some governance, compliance and risk management practices - become a “hinder” rather than a “help”? Are they obstacles to creativity, innovation, entrepreneurship and progress?

The forthcoming Global Convention on Corporate Ethics and Risk Management to be held in Singapore will address the challenge of building an ethical and risk resilient enterprise. It will provide a forum for discussing the board's role, the transition to enterprise risk management (ERM) and how ERM maturity can contribute to value creation. Cyber security issues, ethics, compliance and risk mitigation strategy will be considered from a business building prespective.

The Risk Management Community

What should boards and entrepreneurs make of contemporary risk management? Is it a positive enabler or another compliance cost? Who needs to be involved in it? How conducive of innovation and entrepreneurship are the risk management community and its people in the face of new threats? What needs to change if risk management is to be viewed as less of a hinder and more of a help?

Responsible risk taking is essential for innovation. We need to balance enterprise and control. Do the governance, compliance and risk management communities need to be less of an inhibitor and an expense, and become more of a partner in innovation and a positive contributor of value? In rapidly changing situations, we need to ensure that vision, mission, values, goals, objectives and strategies are still current and relevant. They should be enablers rather than constraints.

Risks rarely recognise our organisational boundaries. The perspectives of some risk managers need to broaden to embrace networks and supply and value chains. Boards should make it clear that they are seeking enterprise and network wide thinking, approaches and responses. They should allocate sufficient time to discuss risk management issues and strategies and come to informed judgements. Should risks be avoided, accepted, mitigated or transfered by means of insurance cover?

We must ensure enterprise and network wide vigilance and responses. All relevant parties should be involved. For example, in relation to fraud and cyber security, specialist expertise must be current and we should look beyond the IT team at the people aspects. Legal and reputational risks relating to breaches also have to be understood and addressed as well as technical and financial issues.

Risks are all around us, including in the air we breathe, but some people seem to concentrate almost exclusively on threats, defences, prevention, protection and continuity. Should there be greater focus upon resilience, recovery, flexibility, reinvention and rapid responses to both threats and opportunities? In many contexts, we may need less stress upon compliance, homogeneity, standards and norms, and more emphasis upon challenge, diversity, bespoke responses and co-creation.

Too many people view risk as negative and a problem. Encountering risk is evidence that you are alive and trying to accomplish something. Governance, compliance and risk professionals must move on from giving advice on how to prevent downsides. Where appropriate, they should also roll up their sleeves and help directors and their colleagues to achieve upsides and collective responses.

Risk managers should become front-line creators of value by turning challenges into opportunities. They must move on from being mainly preoccupied with order, stability, uniformity and standards to exploration, innovation and bespoke and collective responses. Instead of largely reacting to developments, they should actively support decision making and the search for change related business opportunities. They also need to be realists when facing threats such as fraud and hacking.

Identifying Opportunities for Collective Action

Directors and boards cannot afford to be complacent. Being watertight yesterday does not mean one's company will survive tomorrow's cyber

assault. The digital landscape and threats within it are continually changing and evolving. Many companies are struggling to keep up and cope. Is more collaborative action needed? This could range from sharing information to international action.

The most useful anti-fraud collaborators could be equivalent organisations and/or agencies in similar situations in other countries, rather than local companies in one's home country. 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 to cooperate, whether by exchanges of staff, joint working on preventative measures, or addressing particular threats.

Cooperation may or may not be acceptable, depending upon the terms and arrangements. These may specify formats in which data, insights and experiences will need to be captured, stored and transmitted if they are 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 action through trade associations and other bodies can also be helpful.

As well as yielding benefits, collaboration can involve risk. A sharing network itself might be compromised, Staff may be swamped and distracted by an excess of information that might not all 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.

Corporate Obstacles to Progress

The risk of fraud, hacking and failure is sometimes greatest when senior people are at their most confident and others defer to them on account of their past success. From the perspective of law enforcement agencies companies can sometimes be obstacles rather than allies in their attempts to track down and catch criminals. When companies protect their customers' communications and devices from state surveillance agencies this can benefit criminals. Law enforcement agencies may not be able to monitor the activities of suspects and accumulate evidence that might bring them to justice. In some countries, even obtaining court orders cannot open certain devices.

Most directors will instinctively wish 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, and help to bring external parties to justice.

Certain Governments sponsor illegal attempts to secure intellectual property and other information. Companies in sectors such as defence and aerospace may be particularly at risk. They should help their staff to resist attempts to obtain information from them. Some companies that are sensitive to external surveillance by state authorities use various espionage techniques, such as eavesdropping on their commercial rivals. This raises ethical issues that might need to be discussed by a board.

The internet of things creates 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 a fridge might be inconvenient, but unauthorised control of a car could be life threatening. Expensive corporate liabilities could result.

Assessing Probabilities and Prioritisation

Where collaboration occurs and state authorities obtain access to data and communications, there may be other bridges to cross. Although large numbers of frauds may regularly happen, these can represent a small proportion of the large volume of financial transactions that occur 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 the 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 overloaded. 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. A high priority should be put upon protecting customers.

Some threats with low probabilities of occurrence can have large impacts if and when they succeed. An example would be a terrorist attack designed to inflict the maximum of damage and disruption. Simultaneous action against a number of leading banks could be planned 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 would only operate for a limited time without access to credit and/or an inflow of cash, while unrest might occur quickly among unpaid citizens.

Reviewing Corporate Controls

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 continue to try to protect their customers from unwanted intrusion and interference. 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?

Might digital skills training equip future hackers to cause harm? Should it be accompanied by ethical awareness training? Should companies be more circumspect in terms of who receives certain forms of exposure to advanced tools and techniques? 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 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 team should be alert to human factors that might result in hitherto trusted people engaging in fraudulent activities. Should they and others have a remit to protect stakeholders and wider society from illicit activities?

Wider Corporate Responsibilities

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 entities for which they are responsible, or should they acknowledge wider 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?

It might appear that the easiest option is to look the other way and focus upon one's core business, but is this always the right course of action? Data lost in seconds might result in crimes such as identity fraud that individual victims would take many days to address. In such situations, quick action may be needed to protect 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 proactive action where this is legal and appropriately authorised?

Finally, directors and risk professionals should also look at themselves and avoid introversion, denial and excessive risk aversion. They should ensure that they are current and competent in the face of contemporary challenges and opportunities. Curiosity and courage sometimes seem to be in short supply. One wonders where we would be today if more effort had been devoted to developing more resilient systems, quicker responses, more competent directors and more effective boards. ■

***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.*