Focus

- First Reaction
- Governance Spotlight
- Regulatory Overview
- ✓ **Thematic Research**
- Event Based Research
- ✓ **General**

Related research

Primer on the Kotak Committee Recommendations; October 2017

By Invitation

Hiren Shah

hiren@net-square.com

Hiren is a business-and-technology leader with more than 22 years of experience in Capital Markets and IT. Prior to joining Net Square, Hiren has held many senior management positions including as a CIO of CRISIL Ltd. In his role as President of Net-Square, Hiren leads the business strategy, customer relationship and corporate functions. He also acts as a Mentor to the entire team in their delivery.

By Invitation:

Giving IT its due in the boardroom

Going through the recommendations by the Uday Kotak Committee on Corporate Governance (Kotak Committee), I was pleasantly surprised to note two important recommendations. These are:

1. Risk Management Committee (RMC) of a listed company will now be responsible for cyber security also. This recommendation has been made mandatory for the top 500 companies by Market Capitalisation.
2. Listed entities may constitute an Information Technology Committee (TechComm) which, in addition to the risk management committee, will focus on digital and other technological aspects.

Both of them are welcome suggestions. I will, however, recommend one tweak. And that is that even the second recommendation be made mandatory for the top 500 listed companies. My argument for doing that is the same as the argument for having Audit Committee as a mandatory regulation for companies. It is not that the Accounts and Finance department of a company is not competent to report accurate financial position of the enterprise. But financial integrity is very important for sustainability of a business and therefore requires special oversight and hence an Audit Committee. Information Technology (IT) has achieved the same status today and therefore, TechComm should be given the same status as the Audit Committee. If the TechComm is made mandatory, cyber security governance will automatically get covered because this will be high on the list of TechComm's agenda as well.

Now let's look at how should corporates implement these recommendations - starting with the agenda.

In managing cyber security risk, RMCs must form a proactive strategy (most companies today tend to adopt a reactive strategy), which will preempt cyber risks. Beyond the adherence to regulatory and compliance requirements, the RMC must, among other things, undertake a comprehensive threat analysis as a very basic measure to addressing cyber security. I am yet to come across an organisation that does this with sincerity. And many of the threats faced by organisations in application security stem from a lack of this practice.

The agenda of the TechComm, on the other hand, will have to be broader than that of the RMC, since it is required to address a larger agenda of digital and other technology aspects. The TechComm's agenda must include:

1. Enterprise Architecture: The first and foremost agenda for the TechComm has to be to ensure that the technology programs support the business objectives and strategies. The best way to go about this

task is to formalise a program to draw up an Enterprise Architecture. This is particularly vital when an organisation is in a high growth phase and wants to achieve scale without large scale disruption and risk. Earlier, Enterprise Architecture was just the CIO's agenda, but as innovation has gathered pace and technology has become core to business innovation, this agenda has to become a Board matter.

2. Governance of IT investments: Another important aspect of the TechComm should be to govern IT investments. In some ways that would mean tracking whether the IT programs and projects approved by the Board are on track and advising the Board on their progress.
3. Be the people advisor: TechComm's inputs will be very helpful, especially to the CEO, on matters pertaining to staffing of IT / Information Security (IS) functions. As one senior placement professional once put it to me. "IT/IS is like a blackbox for many CEOs and senior business executives. They just ask us to get anyone who has certain years of experience in the domain of their business. They have no way to judge the technical competence of the person". TechComm can fill this gap, especially in the senior level IT / IS hiring. In addition, TechComm can provide an informal input in performance appraisal on a continuous basis of the IT / IS team.
4. Mentor to the technology management team: And on the flip side, members on the TechComm can also be good mentors and advisors to the IT / IS Management team. This comes from my personal experience. Very often, during my stint as a CIO, I wished I could go to a senior Board member and bounce off ideas. Thankfully, my company at the time was part of a global conglomerate and my international colleagues filled that role for me.
5. Be the innovation advisor: It is important that the Board guides the organisation in matters of innovation. And one of the important agenda for the TechComm is to advise the board on new innovations in technology, which needs to be considered by the Organisation whether it be for better serving its own customers or becoming more productive or just to stave off an existential threat before it is too late.

Given the above agenda of RCM and TechComm, let's look at the characteristics of individuals who are ideal candidates to serve on these Committees:

1. IT domain expertise: From my interactions with internal Information Security committees of organisations, I have come away with the impression that they often take the approach of getting external consultants / vendors to provide insights into cyber risk. While this may work in some instances, Boards have to understand that external consultants / vendors may have their own agenda. They cannot be a replacement for having a Board member who will be able to guide the

Board and RMC to answers questions like "Should we implement biometric based banking?" Or "Is blockchain for us?"

The profile of individuals who will be able to do this and help the Board deliver on the agenda should have the experience of managing the technology domain both horizontally and vertically.

Horizontal experience refers to knowledge and experience in the three main domains of technology i.e. IT infrastructure, IT solutions and Information Security. Any challenge, which pertains to cyber security or business solution requires a thorough understanding across all these three domains of technology. Any individual who has mastery in only on one of them will fail in providing a holistic view to solving the challenge.

Vertical experience refers to the ability to assess and provide inputs from strategy to low level architecture. The 'devil is in the detail' indeed – and so, members of the RCM and TechComm should be able to drill down and ask probing questions on how the IT strategy will get implemented.

2. Fourth Dimension is Domain: Some sectors like BFSI, telecom, retail, e-commerce, utilities, healthcare, auto and others may need separate specialists in IT and IS. The challenges posed to these sectors from cyber risks and technology disruptions are more complex than those likely to be faced by other sectors. Just compliance to regulations in many of the above sectors like HIPAA[1], MiFID[2], PCI-DSS[3] etc. adds a significant dimension to the challenge and that requires experience in the particular business domain. Many of the top 500 companies in India operate globally and therefore, they are affected by global regulation and compliance requirements. Considering the larger scope that the RCM and TechComm may have to deal with in these sectors, it may be better to get separate individuals with focused IT and IS expertise in a particular sector.

3. Role of the Internal Team: Senior Risk, IT and IS executives from the organisation who are responsible for day to day operations have an important task of implementing the agenda. All the same, the internal IT / IS Management team should be part of the RMC and TechComm to ensure the link between strategy and implementation is maintained or be answerable to the TechComm. Also for both the RCM and TechComm to be effective they will need continuous feedback and intelligence on the implications of their decisions.

[1] Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers
[2] Markets in Financial Instruments Directive) is legislation for the regulation of investment services within the European Economic Area
[3] The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes

Considering all of the above factors, the individuals best fit for being on the Committee would be career Information Technology (IT) / Information Security (IS) specialists with significant experience in leading or managing Enterprise IT. And they have to be individuals who are daily practitioners in IT/IS. Not just individuals with business experience, even if that is running an IT company. For example, in case of a bank, it can be a professional with a decade plus experience as CIO/CTO in a BFSI organisation.

In conclusion, both the recommendations are a step in the right direction. From stakeholder's perspective, these recommendations will add significant value as IT costs now form one of the highest direct cost elements - maybe only second to material cost or manpower cost.

It is time organisations start considering educating all its directors in matters pertaining technology. At least the terms and jargon used and what these mean. The time to fashionably feign ignorance on a subject that is becoming vital to the very survival of the organization is over, as some of the recent hacks have shown.

Just as Internet has given rise to a new paradigm of "Winner takes all" business models, cyber risks have given rise to a new paradigm "Losers lose all". Perhaps that is the one factor that has prompted the Kotak Committee to make the two recommendations it has. If so, ironical as it may sound, cyber risks have managed to give IT its due place in the Boardroom.

This column is written by Hiren Shah, President and Mentor, Net Square Solutions Private Limited, a company that focuses on managing cyber risks. Hiren can be reached at hiren@net-square.com.

The views in this guest post are those of the author, and not necessarily those of the IiAS Foundation or of IiAS.

Disclaimer

This document has been prepared by IiAS Research Foundation. The information contained herein is solely from publicly available data, but we do not represent that it is accurate or complete and it should not be relied on as such. IiAS Research Foundation shall not be in any way responsible for any loss or damage that may arise to any person from any inadvertent error in the information contained in this report. This document is provided for assistance only and is not intended to be and must not be taken as the basis for any voting or investment decision. The discussions or views expressed may not be suitable for all investors. The information given in this document is as of the date of this report and there can be no assurance that future results or events will be consistent with this information. This information is subject to change without any prior notice. IiAS Research Foundation reserves the right to make modifications and alterations to this statement as may be required from time to time. However, IiAS Research Foundation is under no obligation to update or keep the information current. Neither IiAS Research Foundation nor any of its affiliates, group companies, directors, employees, agents or representatives shall be liable for any damages whether direct, indirect, special or consequential including lost revenue or lost profits that may arise from or in connection with the use of the information. The disclosures of interest statements incorporated in this document are provided solely to enhance the transparency and should not be treated as endorsement of the views expressed in the report.

Confidentiality

This information is strictly confidential and is being furnished to you solely for your information. This information should not be reproduced or redistributed or passed on directly or indirectly in any form to any other person or published, copied, in whole or in part, for any purpose. This report is not directed or intended for distribution to, or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction, where such distribution, publication, availability or use would be contrary to law, regulation or which would subject IiAS Research Foundation to any registration or licensing requirements within such jurisdiction. The distribution of this document in certain jurisdictions may be restricted by law, and persons in whose possession this document comes, should inform themselves about and observe, any such restrictions. The information provided in these reports remains, unless otherwise stated, the copyright of IiAS Research Foundation. All layout, design, original artwork, concepts and other Intellectual Properties, remains the property and copyright of IiAS Research Foundation and may not be used in any form or for any purpose whatsoever by any party without the express written permission of the copyright holders.

Other Disclosures

IiAS Research Foundation is a wholly-owned subsidiary of Institutional Investor Advisory Services India Limited (IiAS), a SEBI registered research entity (proxy advisor registration number: INH000000024).

This page has been intentionally left blank

markets ∩ governance

About IiAS Research Foundation
The IiAS Research Foundation has been established to serve as a platform for business leaders, board members, academics, investors, issuers and intermediaries to interact on the practice of corporate governance and to foster debate around regulations, corporate and investor behaviour and capital markets.

The IiAS Research Foundation operates under three main themes:

I. Research
II. Education and Training
III. Advocacy

About IiAS
Institutional Investor Advisory Services India Limited (IiAS) is a SEBI registered proxy advisory firm (Proxy advisor registration no. INH000000024), dedicated to providing participants in the Indian market with independent opinion, research and data on corporate governance issues as well as voting recommendations on shareholder resolutions for over 650 companies. IiAS provides bespoke research, valuation advisory services and assists institutions in their engagement with company managements and their boards.

In addition to voting advisory, IiAS offers two cloud based solutions - IiAS ADRIAN, and comPAYre. IiAS ADRIAN captures shareholder meetings and voting data and provides packaged data that can be used to gain insights on how investors view specific issues and gain greater predictability regarding how they might vote. comPAYre provides users access to remuneration data for executive directors across S&P BSE 500 companies over a five-year period.

Office
Institutional Investor Advisory Services
Ground Floor, DGP House,
88C Old Prabhadevi Road,
Mumbai - 400 025, India

Contact
solutions@iias.in
T: +91 22 6123 5555