ICGN
International Corporate Governance Network

ICGN Viewpoint

Cyber Risk
May 2016

The issue

Companies and their investors are increasingly concerned about risks associated with misuse of information and communication technology, whether as a result of poor implementation of data systems, missed opportunities to adopt key innovations or failure to protect a business from malicious acts (which are often labelled “hacking” and “cyber” attacks).

Notwithstanding their technical complexities the broad scope and potential gravity of cyber risks are such that these risks must be understood and proactively overseen by company directors as a matter of good corporate governance. This *Viewpoint* report seeks to equip investors to engage with board members regarding cyber risk oversight and cyber related risks. ICGN encourages board members to ask questions to management, proactively, across the entire range of cyber-related risks. Cyber related risks are defined as the range of risks related to information and communication technology that can impede the achievement of company objectives and investor returns.

Investor expectations

The board should encourage steps towards a proactive and mature Information Technology (IT) culture to oversee cyber risks. It is important that cyber risk oversight is integrated with the strategy and risk management of the company, particularly with regard to identifying a company’s critical data and informational assets. Oversight of cyber risks should not be seen in isolation from the technology and business strategy and objectives to which they are related. On the contrary cyber risks should be addressed in an integrated approach across all risks to achieving business objectives.

Board members are encouraged to obtain sufficient knowledge in technology and risk - considering a company’s unique business and structure - to distinguish an appropriate from an inappropriate process, to questions suggested below. As with any business knowledge, investors expect boards to select and train individual board members in cyber risk awareness. This will help board members to provide adequate cyber risk oversight, ask the right questions and understand the answers.

Integrated cyber risk management

Looking back at technology-related risks that caused damage, patterns emerge as to why boards were surprised. Board members did not appreciate the range of risks, speed of change and the need to use the right tools for the job to manage each risk type. With the growth of digital technology comes the growth of risks to business performance related to digital technology.

Companies are clearly vulnerable to cyber-attacks. Examples of cyber-attacks include the recent hacking of several Asian financial institutions. Cyber criminals infiltrated these institutions' computer systems via malware. While these attempts were not all successful, in the case the Bangladesh criminals managed to steal $81 million through the Swift network. While cyber attacks can affect companies in all sectors, the threat of cyber crime in the banking sector has very disturbing knock-on effects, and has made prevention of cyber attacks a priority by regulators including the US Securities and Exchange Commission, the European Banking Authority, the European Central Bank and the Bank of England.

In other cases it is not simply a question of computer hacking. An example of the major impact of wrong implementation of software is Knight Capital, which deployed untested software to a production environment containing an obsolete function. When Knight Capital released the software into production, their trading activities caused a major disruption in the prices of 148 companies listed at the New York Stock Exchange; Knight Capital's stock price collapsed by 70%. The nature of Knight Capital's trading activity was described as a "technology breakdown".

To look forward towards anticipating potential cyber risks, both boards and investors should consider three overarching factors:

1. Risks can be found in four business-technology activities:
    - Product technology strategy, including both the technology in a product or service received by a buyer and technology used to produce it.
    - Business administration and operations technology strategy
    - Programme/project management
    - Daily information technology operations

2. Each of these activities produces risks that emerge in different ways. Thus, each group of risks needs to be addressed with the appropriate approach.
    - Strategic decisions regarding technology should be integrated with broader business strategy and methods of managing risk in the strategy development process (such as overcoming bias) and the plan itself.
    - Technology (software, service, data storage, communications and facilities) should be integrated with broader business operations methods of managing risk to operation objectives such as systems stability, availability, recoverability and protection.

3. In attempting to manage any risk, organizations can easily be overwhelmed and then "surprised" when a risk becomes a serious problem. To more easily manage and mitigate risks, it is helpful to focus on three catalysts of risk -- change, complexity and fatigue (from overheating computers to tired people). The more acute these catalysts, the more time pressure and stress, the more risk. The catalysts apply to anything from pressure to understand technology in an acquisition before a board vote, launch new software, or respond to an infrastructure attack.

Taken together, these illustrate the need for board members to ensure an approach is used that is designed for complex, dynamic environments.

Dialogue with investors

The ICGN encourages companies to enhance communication with investors on how they oversee management activity with respect to cyber related risks. ICGN encourages board members to look at the big picture, across all cyber-related risks to achieving business objectives. Technology is as strategic as selecting the right market for products. Protecting against technology incidents is as much an oversight responsibility as protecting against industrial accidents. ICGN encourages board members to continually improve their personal knowledge of technology and its risks.

In dialogue with board members, investors should be cautious on excessive reactions to the most recent threat or regulatory release; instead the focus should be on a balanced oversight of all cyber-related risks to business objectives. An overly reactive approach often results in using resources in order to fix the most recent crisis – without a proactive, risk-based allocation of resources across all areas of information technology.

Practical questions investors could ask board members related to cyber risk oversight

- How is cyber risk oversight organised within the board?
- How is the board trained and educated to deal adequately with cyber risk oversight?
- How does cyber risk feature in board discussions on 1) strategy process and plan oversight, 2) risk programme management oversight, and 3) risk response readiness?
- How are board meeting discussions managed to avoid the potential of focussing excessively on the last cyber related problem, at the expense of properly anticipating the next problem?

Practical questions investors should encourage board members to ask management across the range of cyber related risks

Strategy process and plan oversight

- How does management assess which of the company's objectives, processes and data are most strategic and most vulnerable to cyber-threat?
- What is the cyber risk security strategy used to manage these risks effectively?
- How is the cyber risk oversight integrated with the strategy and risk mitigation of the company?
- What form of oversight/governance of enterprise information technology is used? How is this linked to strategy and technology investments approved by the board?

Risk programme management oversight

- How is the company improving alignment between business and IT strategy, priorities and budgeting? Does its IT budget map directly to strategic initiative objectives?
- What process discipline is the company following to ensure operationally available, stable, protected and recoverable IT systems? Are these processes in wide use with global and industry education to make it easier to hire, train and improve its people?
- Are employees training with their counterparts in the company's partner and customer organisations on topics such as secure system interconnections?

- How does the company know that resources for managing cyber-related risk are allocated in proportion to each area of risk?
- How does the company understand: 1) any technology that could digitise, demonetise or disrupt its business; 2) technologies that are or will be touching the business model; and 3) exponential technology and the economics of technology on business models in the company's industry?
- What cyber risk is the company managing? Risk to compliance or risk to achieving performance objectives?
- How is the effectiveness of the cyber risk programme evaluated?

Risk response readiness

- How does a company's cyber risk response plan fully address the "what ifs?" and warning signs identified in risk evaluation?
- What was the root cause of the company's last 10 technology problems? Did management use robust approaches to thoroughly diagnose those causes and what is it doing to fix those causes? How was the board involved?

About ICGN Viewpoints

ICGN Viewpoints provide opinion on emerging corporate governance issues and are intended to generate debate, whilst not defining a formal ICGN position on the subject. ICGN Viewpoints are produced by our member-led Policy Committees and we encourage dialogue by contacting Committee chairs directly or the ICGN Secretariat as follows:

Brian Barnier, Co-Chairman ICGN Corporate Risk Oversight Committee: brian@valuebridgeadvisors.com

Carola van Lamoen, Co-Chairman ICGN Corporate Risk Oversight Committee: c.van.lamoen@robeco.nl

George Dallas, ICGN Policy Director: george.dallas@icgn.org