Achieve more effective risk oversight, meet the challenge of cybercrime

Jul 09 2012 Mark S. Bergman and Nitin S. Konchady

A company with an effective risk oversight function could be well-placed to avoid vulnerabilities to cybercrime, and its approaches toward the operational risks it faces would be equally relevant to cybercrime and other threats related to a company's IT infrastructure. These considerations must be analyzed carefully and a broad list of action items for boards and compliance officers should be planned to address a firm's readiness to prevent cybercrime in all of its forms.

A recent op-ed by Preet Bharara, U.S. Attorney for the Southern District of New York, appeared in the *New York Times* on June 3, 2012, and it encapsulates both the risks and the opportunities presented by cybercrime from the perspective of risk oversight.

Mr. Bharara writes that businesses "are not doing nearly enough to protect themselves, their customers and their shareholders." He goes on to say that companies "need to do a better job of creating and fostering a culture of security," and cites a statistic demonstrating that an overwhelming proportion of data breaches are avoidable, which he attributes to failures to take "the most fundamental precautions."

He concludes: "most important step is the most obvious and fundamental one: understanding the threat in a comprehensive, serious manner," and says he fears that too few companies have concrete plans to deal with, or audit vulnerabilities to, cybercrime.

The concern is not confined to the United States. A speech by the Director General of the Security Service (MI5) of the United Kingdom, Jonathan Evans, at the Lord Mayor's Annual Defence and Security Lecture last month addressed the scale of the threat posed by what he characterizes as "industrial-scale processes involving many thousands of people lying behind both state-sponsored cyber espionage and organized cybercrime."

Evans notes that a major London listed company estimates that it incurred revenue losses of around £800 million as a result of a cyber attack, not just through intellectual property loss but also from commercial disadvantage in contractual negotiations. He went on to say that the boards "should consider the vulnerability of their own company to these risks as part of their normal corporate governance – and they should require their key advisors and suppliers to do the same."

Defining the risk oversight function

For directors and compliance professionals seeking to better understand their role, the key is to understand the difference between risk oversight and risk management. A set of action items is provided below.

Although there is no uniform definition of risk oversight, there are common elements. The function certainly involves understanding the key risks the company currently faces and could face in the future. The function should involve an ongoing dialogue with management regarding risk appetite and whether strategy is consistent with risk appetite. Finally, the function requires an understanding of management's risk management procedures and monitoring of the effectiveness of risk management procedures.

Risk management on the other hand describes the initiatives of management to: (a) identify, quantify, monitor and report, and mitigate the key risks to the business, its corporate strategy and the implementation of that strategy, (b) help establish, and then communicate to the organization, the risk appetite, and (c) establish the proper risk culture. Central to this endeavor will be the parameters set around risk appetite and risk tolerance.

A critical element of risk oversight is the board's structure for overseeing risk. While the full board typically will, as a matter of corporate law, have overall responsibility for this task, risk oversight responsibilities often are delegated to one or more board committees. While many companies outside the financial services industry locate the risk oversight function in the audit committee, there continues to be an ongoing debate as to whether boards should establish separate committees tasked with taking the lead on risk oversight, and an increasing number of companies are doing so – in the form of "risk committees" or "finance and risk committees."

Others have established committees that focus on complex risks unique to the particular company, whether it is technology, science or safety, for example.

Boards that establish risk committees should ensure that committee members have the requisite industry knowledge and experience and that there is appropriate coordination with other committees, in particular the audit committee.

Board action items

Effective risk oversight should not be viewed as a check-the-box exercise or as a static undertaking. With ever-changing risk landscapes, risk management structures should be tested regularly to ensure they are evolving as risks evolve, and risk oversight needs to take account of the dynamic nature of the challenges management teams will face. For directors wishing to better understand their risk oversight role, a list of action items is set forth below.

1. Determine the appropriate board-level structures to address risk oversight – full board; delegation to audit committee; risk committee.
    - Note that different businesses require different approaches.

- Note that while risk oversight is a board responsibility, certain functions can be delegated to one or more committees.

- Consider whether enough time is allocated to risk oversight matters, particularly when this includes discussions of strategy and risk appetite.

2. Evaluate the skill set at the board level; consider benefits of board turnover; consider maintaining "director turnover" lists detailing potential board candidates, their qualifications and other attributes; consider the benefits of board diversity; and consider the ability to have candid discussions and to ask the tough questions.

    - Note that there is no universal agreement on the right skill set.

    - Note too that those tasked with risk oversight, particularly for companies with complex and fluctuating risk profiles, will likely need expertise and experience that differ from the expertise and experience that make for an effective member of the audit committee.

3. Evaluate the potential benefits of a chief risk officer (CRO) and the CRO's potential mandate.

    - Note that the CRO can provide input on strategy.

    - Note that the CRO should in any event facilitate aggregation of risk data.

    - Note too that the CRO should have the requisite mix of experience and skills.

    - Consider what the proper reporting lines for the CRO should be in light of the company's governance structure.

4. Understand the broad universe of risks and the most significant risks; understand that risks can be strategic or operational. Although there are different ways of categorizing risks, they are likely to include:

    - Competition

    - Customer

    - Supply chain

    - Market

    - Credit

    - Counterparty

- Financial
- Regulatory and compliance
- Information technology (including security of customer and proprietary data, overall vulnerability to cyber threats and risks posed by the pervasive use of social media)
- Human resources
- Health and safety

5. Understand the difference between risk management and risk oversight; articulate an approach to risk oversight that is appropriate for the company and its business – based on acceptable risk appetite, complexity of the risks the business faces and the regulatory environment.

6. Evaluate the company's risk appetite and its relationship to strategy; communicate the board's view of the company's risk appetite and ensure that the message is communicated throughout the company.
   - Note that all enterprises have a risk appetite; they may not characterize it as such.
   - Recognize that not all risks are measurable.
   - Evaluate the risks that are acceptable and the ones that are not, and set the risk tolerances on that basis; agree on acceptable frameworks for evaluating the enterprise's risk appetite and the appropriate limits. For example:
     - What limits are imposed in connection with the launch of new products, penetration of new markets or conducting business in new countries?
     - What are acceptable levels of debt?
     - What parameters are in place in respect of hedging arrangements?
     - What is deemed to be an acceptable negative impact on earnings?
     - What are appropriate target financial ratios or target credit ratings?
     - What are the minimum conditions for organic growth versus growth by acquisition, or joint ventures?

- What are acceptable headcount levels given the enterprise's existing infrastructure, and what levels would be required as the enterprise grows?
- What are acceptable sources of financing?
- What are appropriate levels of research and development activities?
- What are the implications of customer concentration?
- What are the implications of competition?
- What limits are applied to insurance arrangements, including captive insurance programs; how might risk transfer and capital management coverage benefit the company?
- What is the acceptable level of corporate political activity, including limits, if any, on contributing corporate funds to political campaigns?

7. Understand management's risk management processes and how those processes are applied across the enterprise. Remember that significant risks to the enterprise may arise in smaller business units or in other unexpected (or remote) areas of the business.
   - Pose the "what if" questions and challenge existing assumptions.
   - Pose the "can this happen to us" questions.
   - Consider how deviations from risk limits are handled.
8. As emphasized in the most recent progress report issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), periodically evaluate whether developments in the risk landscape have been factored into risk management assessments and strategic decisions. Changes in market conditions, the mix of business, the competitive landscape, the legal or regulatory landscape, macro-economic conditions and the geopolitical situation, to name a few, can have an impact on risk considerations, and hence on strategy and business plans.
9. Assess the way in which the board seeks to perform its risk oversight function; consider the timing and content of management reporting to the board on risk; ensure there is agreement with management on what should be elevated to the board, when and in what form; and be aware that potentially significant risks may not at first be obvious. Consider in particular the way in which information is communicated upward, and whether the aggregation of information in the form of summaries or presentation slides adversely impacts the ability to comprehend the information.

- Is the board fully satisfied with the monitoring and reporting of risks to the board?
- Is sufficient time allocated to risk oversight matters?
- How frequently are the most significant risks reported to the board?
- How frequently are management's processes and procedures reviewed?
- How frequently are emerging risks and the changing landscape discussed with the board?
- To what extent are risks measured on an aggregated basis?
- How frequently are gap analyses (*i.e.*, an evaluation of the gap between actual and potential performance) performed and reported to the board?
- How frequently are "remote" risks and worst-case scenarios analyzed and reported to the board?
- Does the board assess the level of resources devoted to risk management?
- If risk limits are exceeded, when are these circumstances reported to the board?
- Has the board addressed crisis management procedures?

10. Obtain external perspectives, particularly in respect of global operations and emerging risk areas, including:
    - Presentations by auditors, outside counsel, risk consultants or business intelligence firms.
    - Research reports covering the company, its competitors and the industry.
    - Summaries of public disclosure of competitors.
    - Recommendations of shareholder advisory firms.
11. Reach out to others in the company beyond the CEO, chief financial officer and CRO to get a sense of the risk culture and test risk assumptions.
    - Note that input is likely needed from heads of business units, the chief legal officer, auditors, and the heads of information technology, human resources and investor relations.
    - Evaluate the escalation processes for reporting risks to senior management and the board?
12. Recognize the overriding importance of "tone at the top."

- Risk considerations should be integral to business planning, including expansion of the business into new products, new markets and new countries and expansion through acquisitions or joint ventures.

- Responsibility for risk management should be clearly defined and consistently applied across the enterprise.

- Sufficient resources (with the requisite experience and skills, and the requisite authority) should be allocated to risk management.

- Management should be proactive in involving the board and CROs in risk management as it pertains to the firm's business planning overall.

- Management needs to communicate that it fully embraces risk management and fully appreciates the importance of risk management processes.

- There should be a culture of open dialogue and candor; red flags should not be ignored; potential issues should be timely escalated to the proper levels.

- Adherence to risk limits and risk tolerances should be factored into compensation and promotion decisions; failure to adhere must be properly addressed.

- Management should follow up on identified gaps.

- Internal compliance programs (to address fraud, bribery, regulatory compliance and the like) and whistleblower programs should be robust and evaluated on a periodic basis; directors, senior management and other employees should receive the appropriate level of training and have access to relevant, clear and concise compliance guidelines.

- Directors should be mindful of reporting obligations to the board under applicable ethics and compliance requirements, such as the U.S. sentencing guidelines.

13. Consider whether the company has succession plans in place, particularly to address unexpected departures of senior executives.

14. Consider whether existing channels for engagement with shareholders are effective.

15. Ensure that the enterprise has contingency plans, with well-defined crisis management protocols and communications strategies.

16. Evaluate the board's risk oversight efforts.

17. Recognize that risk oversight and risk management are important issues for shareholders and that in addition to a range of other corporate governance areas, risk oversight will be assessed by the proxy voting services. The importance of effective risk oversight processes was underscored in late 2011 by the expansion by Institutional Shareholder Services of the factors that it will consider in recommending votes against or withhold votes for directors to specifically include material failures of risk oversight.

Risk oversight and cybercrime

In an era when business has become more global and more complex, laws and regulations often are becoming more restrictive and bad news can go viral in an instant, risk oversight and risk management must be uppermost in the minds of corporate directors and management. These functions must be dynamic, as the risk landscape will shift over time.

Risks faced by companies naturally will depend on the nature of the company and its operations, and yet certain risks will apply across the board. Returning to the theme of risks posed by cybercrime, it is difficult to imagine a company today that is not heavily reliant on information technology and thus vulnerable to cybercrime. One should expect then that at a minimum directors of most companies feel comfortable that they understand:

- How the company uses IT.

- Whether the use of IT is compliant with applicable laws and regulations, which can cover a range of areas from compliance with data privacy requirements, trademark and copyright laws, employment laws and regulations.

- Whether management assesses the company's compliance with contractual obligations related to cyber security.

- Whether management assesses the company's ability to comply with document retention policies and respond to litigation "holds."

- Whether management assesses the impact of changes in technological innovation.

- Whether the IT budget is properly deployed.

- Risks associated with outsourcing.

- Risks associated with cloud solutions.

- Risks of loss or theft of sensitive information, and general vulnerability to cyber threats; whether the company is

able to discover a cyber attack; how management expects to respond to a cyber attack (including its readiness to involve law enforcement agencies); and how management remains informed of cyber threats. (In this area, SEC reporting companies now have SEC guidance on enhanced cyber security reporting requirements.)

- Whether management conducts employee training and periodic threat assessments, including independent audits, in relation to the company's IT systems and the vulnerability of those systems to external as well as internal threats.

- Whether the company's insurance coverage covers cyber-related risks.

- Risks of significant adverse effects on brand or corporate reputation through social media communications, whether from dissatisfied customers, competitors or disaffected employees, and how the company will respond if the risks come to fruition.

While strategic risks may be more abstract, the threats to most businesses posed by failures of information technology – ranging from a crash of a mission-critical system, to theft of proprietary information, theft of customer data or outright sabotage – should serve as a useful reminder of the importance of robust risk management procedures and the roles directors can play through effective risk oversight to minimize failures of risk management.

Mark S. Bergman *is a partner, Paul, Weiss, Rifkind, Wharton & Garrison LLP, resident in London and co-head of the firm's Capital Markets and Securities Group.* ***Nitin S. Konchady*** *is an associate in the firm's Capital Markets and Securities Group.*