BoardroomDirect

The monthly newsletter for PwC's Center for Board Governance – April 2013

Inside this edition (April 24, 2013)

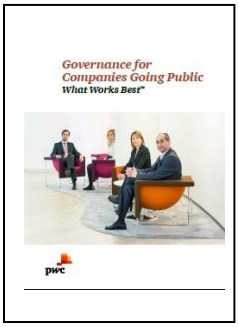
Latest Center for Board Governance publication

The quarter close Directors -- edition Q1 2013 focuses on the trend of stock buybacks at companies with excess cash, a preview of the 2013 proxy season, leadership changes at the SEC and FASB, and key decisions on the revenue recognition project.

Worth reading

Reaching greater heights: Are you prepared for the journey?
Many companies' internal audit departments are not keeping up.
-- PwC 2013 State of the Internal Audit Profession Study

IPOs and governance for directors webcast



PwC's Deals practice hosts a webcast from 1-2 p.m. EDT on April 25 on today's IPO environment: changing market conditions, new expectations for board members, and what you need to know about MLPs (master limited partnerships). Speakers include Mike Gould, Partner, Deals, PwC; Joe Dunleavy, Partner, Deals, PwC; Catherine Bromilow, Partner, Center for Board Governance, PwC; and Derek Thomson, Director, Deals, PwC. To register, click **here**.

Resources, webcasts, and events

The latest offerings from the PwC Center for Board Governance. Click here.

Contact us

For more information or to submit feedback about this newsletter, contact Gary Larkin (gary.p.larkin@us.pwc.com).

Issue in focus

Cybersecurity risk on the board's agenda

Back to top

As the number of database breaches, company web site hacks and loss of intellectual properties grows, company boards realize cybersecurity is not just a technology risk. It can be an enterprise risk management issue.

What's at stake for companies are their so-called "crown jewels," those information assets or processes that, if stolen, compromised, or used inappropriately would render significant hardship to the business.

Cybersecurity issues are among the top risk management issues facing companies, according to recent surveys by PwC. The PwC *2012 Annual Corporate Directors Survey* of 860 public company directors found that nearly three-quarters (72%) of directors are engaged with overseeing and understanding data security issues and risks related to compromising customer data.

"Today, cyberthreats are a real danger to the global business ecosystem," said Peter Harries, Leader, PwC Health Information Privacy and Security Practice. "Yet many enterprises place the responsibility for managing cyberthreats solely in the hands of their technology team. Now is the time for boards and management to realize such threats are enterprise risk management issues that could severely affect their business objectives."

The sheer volume and concentration of data, coupled with easy global access throughout businesses in the US and worldwide, magnifies the exposure from a cyberattack, according to a PwC *10Minutes on the stark realities of cybersecurity*. Such attacks often originate from three areas: nation-states, organized crime and "hactivist" communities, according to Harries.

"Nation-states are trying to achieve a certain outcome, such as the illegal acquisition of intellectual property or competitive intelligence," he said. "In the case of organized crime, they are looking to make money from information, such as healthcare and credit card information. Hactivists want to raise awareness on a social policy issue with disruptive responses, such as a denial of service attack."

Additionally, recent data from PwC's 16th Annual Global CEO Survey found that more CEOs in the US (31%) believe a cyberattack or major disruption of the Internet is likely to occur than global CEOs (20%). In February, President Obama issued an executive order to improve critical infrastructure cybersecurity.

That executive order calls on federal agencies to strengthen US cyber defenses by sharing more public-private information, identifying and prioritizing US critical intellectual property (IP) infrastructure, and building a cybersecurity framework. The order, which impacts the Department of Homeland Security, the Department of Commerce's National Institute of Standards and Technology, and the Office of the Director of National Intelligence, is going to take effect in phases from June through August**. [For more information and a timeline on**

the order's phase-in, read PwC's *Cybersecurity and Corporate America: Finding Opportunities in the New Executive Order*.]

The order requires the private sector and government to share critical information for those 18 industries deemed "critical infrastructure." A crucial part of the order calls for building a framework that will include standards and best practices to be used by companies to defend their IT networks against cyberattacks.

"We've reached a tipping point for the government sharing critical information with the public," David Burg, PwC's US Leader of Forensic Technology Solutions, told Bank InfoSecurity at the 2013 RSA Conference in an interview. "We have reached a phase where we need to institute a cyber immune system to help our commercial industries, or those at a minimum considered to be critical infrastructure, to have much more rapid access around threat information to enable our economy to respond and to reduce the threats."

In October 2011 the SEC's Division of Corporation Finance released guidance regarding cybersecurity risk disclosure that states companies "should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents." While there are no disclosure requirements that specifically discuss cybersecurity, the SEC guidance states that companies should disclose cybersecurity risks in the risk factor disclosures consistent with Regulation S-K Item 503 (c) and address such risks in other areas of their filings, including Management's Discussion & Analysis.

What should directors do

As boards consider how to prepare for and react to cyber attacks, there are certain considerations they should make related to data security, according to PwC's *Directors and IT: What Works Best* ™ board guide:

- **Determining the effectiveness of the company's security program –** Evaluate if the company is effectively addressing data security, understand the company's perceived level of data security risk and the controls designed to mitigate the risk, and consider whether a chief information security officer (CISO) is needed. If so, ensure that person has appropriate stature in the company.

- **Leading practice is to have a data security approach that is comprehensive and adequately funded –** Understand the company's comprehensive strategy for addressing data security, determine how management tests resistance to attacks, and ask management about the company's IT security resources and whether the security spend level is appropriate.

- **Detection can be a problem –** Discuss the frequency and incidence of data attacks the company has detected in recent years and how the company responded.

- **Protecting the most sensitive and valuable assets –** Inquire about the company's inventory of sensitive information, including IP, and the controls to protect it.

- **Concerns outside the company's firewall –** Ask management if and where sensitive information is housed outside the company and how it is protected.

- **Internal employee risk cannot be overlooked –** Understand how the company educates employees about data security risks and the related policies and procedures.

- **Compliance and regulatory risks are rising –** Discuss with management whether the company's disclosures are appropriate and ask about the latest data security regulations.

For more information on cybersecurity risk, directors also may want to read the following publications:

- PwC: *Directors and IT: What Works Best™, Part 2 – IT Subjects, Data security*

- *New York Law Journal*: Cybersecurity Risks and the Board of Directors

Issues in brief

SEC: Social media use OK under Reg FD, if investors are alerted

Back to top

Earlier this month the SEC clarified that its 2008 guidance regarding companies' use of websites to disseminate information to investors applies to the use of social media.

Following a report of investigation, the commission announced that companies can use social media outlets like Facebook and Twitter to announce key information in compliance with Regulation Fair Disclosure (Reg FD) so long as investors have been alerted about which outlet the company will use. **[Read the SEC's press release on the social media announcement here.]**

"Companies should review the commission's existing guidance," Lona Nallengara, acting director of the SEC's Division of Corporation Finance, said. "It is flexible enough to address questions that arise for companies that choose to communicate through social media, and the guidance does so in a straightforward manner."

Reg FD requires companies to distribute material information in a way that is broad and non-exclusive. It is designed to ensure that all investors have equal access to that information at the same time.

For more information on social media risks, directors may want to refer to the BoardroomDirect January 2013 *Message to directors: Get more social in the IT space* brief.

US Chamber puts forth proxy advisor principles

Back to top

An arm of the US Chamber of Commerce is calling for more disclosure and transparency by the two major proxy advisory firms (Institutional Shareholder Services and Glass Lewis).

In its recently released Best Practices and Core Principles for the Development, Dispensation, and Receipt for Proxy Advice report, the US Chamber of Commerce's Center for Capital Markets Competitiveness calls for proxy advisors to share drafts of their work with public companies. The report also asks that the advisory firms adopt policies and procedures that ensure the accuracy of their research and disclose potential conflicts of interest.

In the report, the Chamber states that it wants these principles to serve as a basis for proxy advisory firms, public companies, and investment portfolio manager organizations to engage in a dialogue to create a system that fosters strong corporate governance.

"The system is broken and it is time to fix it," said David Hirschmann, president and CEO of CCMC. "The voting standards and advice issued by proxy advisory firms need to be grounded in fact and reflect reality. As the number and complexity of issues on the proxy has grown exponentially, proxy advisory firms have failed to develop open, clear and evidence based standard setting systems to help ensure the advice they provide strengthens corporate governance and shareholder value."

The Chamber also believes that its guidelines are a start to creating the transparency, accountability and good governance needed to achieve those goals, Hirschmann said.

Representatives of ISS and Glass Lewis did not seem very receptive to the Chamber's principles and statements.

"As a firm committed to helping institutional investors exercise their fiduciary duties, ISS could not disagree more with the US Chamber of Commerce's assertions that the corporate governance system is broken," according to an ISS statement. "We take exception with the chamber's misinformed characterization of the proxy advisory industry..." The statement reiterated that ISS is accountable to its clients, companies they analyze and the regulators that set the guidelines for fiduciary responsibility.

Robert McCormick, Glass Lewis chief policy officer, told Reuters that some points raised by the Chamber could be acceptable. **[Read *US Chamber of Commerce wants more proxy advisory disclosures*.]** While he agreed with the need to disclose potential conflicts of interest, he said other principles, such as sharing research with companies before being published, were "non-starters."

Audit committee issues

Should audit committees ask more of their internal auditors?

Back to top

With market volatility, complexity, and ongoing political and regulatory changes, internal audit (IA) functions have more opportunities to contribute to businesses in a meaningful way, according to the *PwC US Internal Audit State of the Profession 2013 survey*.

According to survey respondents, internal audit must continue to evolve its focus and significantly improve its performance or risk losing relevance as other internal risk functions become more vital contributors in the risk management area.

According to the survey, audit committees and management should ask if they are expecting enough from IA or if they are settling for a function that audits to their capabilities and not to their risks.

The survey also found that there is a huge opportunity for internal audit functions to be relevant contributors to protecting stakeholder value and the business from the most critical risks. However, for internal audit functions to maximize their value to the organization, they must ensure alignment on multiple levels.

The survey also outlines the key steps audit committees can take to enhance the value internal audit can and should deliver to organizations. Those steps include audit committees asking:

- If the expectations it has set for internal audit are clear enough and high enough.
- If critical business risk coverage is aligned with its views on risk.
- If internal audit has a strategic plan and the resources it needs to deliver value.
- If the audit committee is enabling internal audit to be what it should be.

NYC attorneys group ask NYSE to reconsider audit committee risk rule

Back to top

The New York City Bar's financial reporting committee has asked the New York Stock Exchange to reconsider its 2003 rule that requires audit committees to discuss policies regarding risk assessment and risk management.

The attorney group, which has more than 24,000 members, believes risk assessment and management oversight should be elevated to the whole board, It is concerned about how much this rule has increased the workload of audit committees and that there is a lack of clarity over audit committees' responsibility regarding risk oversight.

"We would encourage the NYSE to revisit whether Rule 303A.07 reflects an optimum approach to board-level oversight of risk management," the Bar said in a March 5 letter to the NYSE's regulation arm. "In particular, we would ask the NYSE to consider that, while audit committees should certainly retain responsibility for the oversight of those risks associated with financial reporting, the audit committee should not be required to assume broader risk management oversight responsibility."

The Bar goes on to state that if the whole board was required to "discuss policies with respect to risk assessment and risk management" then the whole board could use its judgment to delegate certain or all aspects of risk management oversight to the audit committee or other committees as the board deemed appropriate.

NASDAQ proposes internal audit function requirement

Back to top

The NASDAQ Stock Market recently filed with the SEC a proposed rule that would require listed companies to establish and maintain an internal audit function that would go into effect the end of this year. Currently, the NYSE has such a requirement.

If approved, the rule would require listed companies and those listed on the exchange before June 30 to establish an internal audit function by December 31, 2013. For those companies listed after June 30, they would have to have such a function prior to listing.

Under the proposed rule, the company may choose to outsource the function to a third-party service provider other than the independent auditor. Also, the rule would require the audit committee to:

- Meet periodically with the internal auditors and assist the board in its oversight of the internal audit function performance

- Discuss with the independent auditor the responsibilities, budget and staffing of the internal audit function

As of April 4, there have been 35 comment letters filed with the SEC. A large majority of the letter writers (27) are against the rule, while only three are in favor. There were four that asked it be amended to either exempt smaller companies or specify that there be an emphasis on an effective internal audit function.

Of those against the rule, the Society of Corporate Secretaries and Governance Professionals writes: "We suggest that the proposed rule: (1) be clarified to limit its scope to financial reporting risk and internal controls over financial reporting risk only; (2) allow outsourcing of the internal audit function to multiple providers (whether or not the scope is limited); and (3) have an effective date no earlier than the end of the first full calendar year following the year in which the rule is approved."

The Institute of Internal Auditors (IIA) writes that the organization supports the internal audit function requirement, but that it recommends the rule require such functions "follow globally recognized professional standards." It also states that it is best practice for audit committees to periodically hold a private executive session with the chief internal audit executive without management present.

COSO to issue updated framework in May

Back to top

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission announced at its March 20 meeting that it expects to issue its updated *Internal Control – Integrated Framework: 2013.* Also, the framework will include a volume of *Illustrative Tools for Assessing Effectiveness of a System of Internal Control.*

Additionally, COSO expects to issue simultaneously *Internal Control over External Financial Reporting: A Compendium of Approaches and Examples,* which has been developed to assist users when applying the *Framework* to external financial reporting objectives. The framework compendium was written by PwC as part of the framework update. It illustrates how the principles in the framework can be applied in designing, implementing and conducting internal control over financial reporting. **[To read the draft versions of the compendium, the revised framework, and the illustrative tools, click here.]**

The COSO board also announced that it will continue to make available the original framework during the transition period extending to December 15, 2014, after which time COSO will consider it as having been superseded.

For more information on the updated COSO framework, directors may want to read page 3 of the March 21 ***PwC Flashline***.

PCAOB to consider proposal for auditing standards reorganization

Back to top

On March 26 the Public Company Accounting Oversight Board (PCAOB) issued for public comment a proposal for the reorganization of PCAOB auditing standards, as well as certain related amendments to its rules and standards.

Among the proposed changes, all PCAOB auditing standards would be grouped into the following categories: general auditing standards, audit procedures, auditor reporting, matters relating to filings under federal securities laws, and other matters associated with audits.

Comments on the proposal are due by May 28, 2013.

For more information about the PCAOB auditing standards proposal, directors may want to read PwC's March 29 *In brief: PCAOB proposes framework for reorganization of PCAOB auditing standards.*

Resources, webcasts, and events

Back to top

The quarter close – Directors edition Q1 2013: This edition focuses on leadership changes at the SEC and FASB, key decisions on the revenue recognition project, the FASB's latest proposals on financial instruments, latest FASB releases and updates on key standard-setting projects, recent SEC, PCAOB, and IFRS developments, and corporate governance matters, including a preview of the 2013 proxy season. **To read the publication, click here.**

Center for Board Governance Webcast Archive: The archive of the April 16 quarterly webcast that focused on the board's role in the strategy and oversight of capital projects and other significant transactions is available. **For more information and to view, click here.**

PwC's Board Center App: PwC's Board Center App provides timely insights on corporate governance issues and trends to enable board members to more effectively meet the challenges of their critical role. Available for the iPad, the app provides access to our full library of publications and on-demand videos. **Download the Board Center App.**