to the point

Winter 2013

Current issues for boards of directors

pwc

In this issue

Clarifying the FCPA

The Foreign Corrupt Practices Act (FCPA) prohibits US companies and citizens (and certain non-US companies) from paying foreign government officials to help obtain or retain business. The FCPA also requires companies whose securities are listed in the United States to maintain adequate books and records that accurately and fairly reflect all transactions. The Securities and Exchange Commission (SEC) and US Department of Justice (DOJ) use these requirements to prosecute companies on anti-bribery charges.

For its year ended September 30, 2012, the SEC reported that it had filed 15 enforcement actions for FCPA violations. And its fiscal 2012 whistleblower report included 115 whistleblower tips related to the FCPA. Although the number of cases may be small, the settlements are usually large. Since 2009, regulators have entered into more than 50 settlements and plea deals with companies relating to the FCPA, resulting in more than $2 billion in penalties.

SEC and DOJ issue new guidance

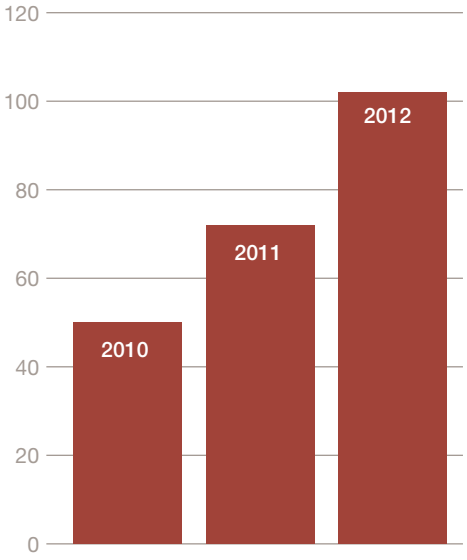
In late 2012, the SEC and DOJ released *A Resource Guide to the U.S. Foreign Corrupt Practices Act* to help companies and individuals comply with the law, prevent and detect FCPA violations, and implement effective compliance programs. The guide might be particularly useful to smaller companies that have less experience with the law and fewer resources to educate employees and prevent violations.

The 120-page guide summarizes FCPA cases, includes examples of enforcement actions, and describes situations where the SEC and DOJ declined to pursue an allegation. It also

- Explains the elements of a violation and defines who is a foreign official
- Outlines the hallmarks of an effective compliance program and how such a program helps mitigate penalties
- Explains the vulnerabilities associated with a company using foreign agents
- Describes what is and is not a facilitating payment
- Provides guidance on gifts, entertainment, and travel expenses, particularly what is proper and improper
- Addresses liability when a company merges with or acquires another company with FCPA issues

continued on page 4

Cyberattacks—it's not a matter of if, but when



Source: *2012 Cost of Cyber Crime Study*, Ponemon Institute, October 2012.

In today's technologically reliant society and business world, data security is increasingly a top concern for directors. Mobile computing, the cloud, and social media have created even more security risks. Why? Because they allow greater data access from outside traditional corporate firewalls and more easily accommodate complex data threats. Worms, viruses, and hackers have become more sophisticated, and all present threats to a company's data security.

The frequency of cyberattacks is growing: Organizations experienced a 42% jump in the number of cyberattacks in 2012, with an average of 102 successful attacks per week.[1] Cybercriminals not only seek personal and financial information, they are also after intellectual property and trade secrets, which often represent tremendous value to a company.

What does this mean for companies and directors?

It is a given that cyberattacks will occur and that the company cannot completely eliminate all cyber risks. Companies should prepare for the inevitable by assessing their data security programs. A well-developed security strategy that includes processes to monitor networks, computers, and user access can help identify potential threats, mitigate fraud, and protect shareholder value and brand image.

Even when companies recognize their IT risks, many lack an overall information security risk management strategy. This strategy should be unique to each company's facts and circumstances and reflect the nature of the company's information assets. Some companies conduct their own security tests to determine their vulnerability to attack, and others hire outside security organizations to perform them. For their part, directors should understand the company's perceived level of data security risk and the controls designed to mitigate the risk. It's also important for boards to discuss with management if and where sensitive information is housed outside the company, including how information housed in the "cloud" is protected.

Even with a security strategy in place, companies are not necessarily effective at detecting breaches. Security breaches often go unnoticed for long periods of time: 86% of the data breaches studied in 2011 were discovered not by the victimized organization, but by external parties like law enforcement.[2] Directors should ask how the company monitors for breaches, how frequently data attacks occur, who is behind the attacks, and how the company responded.

Risk doesn't only come from the outside. "Trusted" internal users—employees, contractors, or other insiders—can also present security risks. These users are generally well-meaning, but may not always follow the company's controls and procedures. There may also be the risk of a disgruntled employee who purposefully violates company policy and security protocols. So directors should also understand how the company educates employees about data security risks and the related policies and procedures. This should encompass the protocols regarding portable and mobile devices, as well as the use of social media.

For more, see PwC's guide, *Directors and IT—What Works Best, A user-friendly board guide for effective information technology oversight*.

1 *2012 Cost of Cyber Crime Study*, Ponemon Institute, October 2012.

2 Wade Baker et al., *2011 Data Breach Investigations Report*, Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit.

ISS's proxy voting policy updates for 2013

In our *2012 Annual Corporate Directors Survey*, 61% of directors indicated they believe proxy advisory firms' recommendations influence over 20% of the voting results. So directors will likely be interested in the key proxy voting policy changes that proxy advisory firm Institutional Shareholder Services (ISS) announced in November for the 2013 proxy season.

Executive compensation

Peer groups

In the past, ISS used the S&P Global Industry Classification Standard (GICS) to select peer groups for compensation comparisons. Some companies were concerned this approach resulted in peer groups that didn't always include the multiple business lines in which the company operates, and that it sometimes omitted direct competitors or otherwise led to inappropriate comparisons.

In 2013, ISS will consider a company's self-selected peer group, as well as look to market capitalization, revenues, and GICS code peers. ISS will prioritize peers that put the company in the mid-range of the group, those that are in the company's chosen peer group, and peers that have chosen the company itself as a peer.

Realizable pay

ISS will add the consideration of realizable pay into the qualitative analysis of compensation for large-cap companies. Realizable pay is the sum of the value of in-the-money stock options and full-value equity awards at the end of a performance period. ISS acknowledges that the realizable pay consideration may make CEO's pay-for-performance comparison appear better for some executives and worse for others.

Golden parachute proposals

The Dodd-Frank Act requires companies to hold separate shareholder votes on potential "golden parachute" payments when they seek approval for mergers, sales, and certain other transactions. When considering say on golden parachute vote recommendations, ISS will now consider any existing change-in-control arrangements with named executive officers, rather than focusing only on new or extended arrangements.

Board response to majority supported shareholder proposals

Starting in the 2013 proxy season, ISS will recommend voting against individual directors or the entire board if the board fails to act on a shareholder proposal that received the support of a majority of the shares *outstanding* the previous year or the support of a majority of the shares *cast* the last two out of three years.

Then in 2014, ISS will recommend against individual directors or the entire board if the board failed to act on a shareholder proposal that received support of a majority of votes *cast* in the previous year alone.

ISS indicates it will review board responses involving less than full implementation of a shareholder proposal on a case-by-case basis, considering disclosed shareholder outreach efforts and board actions to engage with shareholders, among other factors.

Hedging and pledging of company stock

Beginning in 2013, ISS's policies will change on hedging and significant pledging of company stock by directors and/or executives. It will consider *hedging* any amount of company stock to be a "problematic pay practice" and will issue a negative voting recommendation against appropriate board members. ISS will take a case-by-case approach in determining voting recommendations for directors at companies where directors or executives *pledge* company stock. It will consider the company's policies to prevent pledging in the future, and the magnitude of pledged shares compared to shares outstanding, market value, or trading volume, among other factors.

Clarifying the FCPA

continued from page 1

The guide suggests a number of possible risk-based compliance controls, such as:

- Devoting greater resources to the review of large contracts in high-risk regions than to modest entertainment and gift giving
- Implementing web-based approval processes for gifts, travel, and entertainment that give senior management or in-house counsel an opportunity to review requests in advance
- Providing a mix of training opportunities and materials, including materials translated into local languages and customized for particular functions
- Publicizing disciplinary action within the company to demonstrate the consequences of misconduct and openly rewarding contributions to the company's compliance program

What directors should know and do

Directors should be aware of the new guidance and ask their compliance officers how the company's compliance program and training will be updated to reflect these clarified expectations. This is particularly important given that robust programs to educate employees, distributors, agents, and resellers can help minimize the risk of enforcement action or severe penalties.

Directors will also want to discuss with the company's compliance officers or general counsel whether the company is vulnerable to the types of violations the government is focusing on and what is being done to minimize those risks.

Note to readers: This will be the last edition of *To the point*. Future content can be found in our monthly e-newsletter, *BoardroomDirect*.

How PwC can help

To have a deeper discussion of how these subjects might affect your company or board, please contact:

Mary Ann Cloyd
Leader, Center for Board Governance
973 236 5332
mary.ann.cloyd@us.pwc.com

Catherine Bromilow
Partner, Center for Board Governance
973 236 4120
catherine.bromilow@us.pwc.com

Don Keller
Partner, Center for Board Governance
512 695 4468
don.keller@us.pwc.com

You may also want to see

2012 Annual Corporate Directors Survey

Significant changes in corporate governance are impacting boardroom dynamics, compelling directors to spend more time on board work and prompting them to reconsider their oversight approach. Our *2012 Annual Corporate Directors Survey* outlines progress directors have made in their roles and challenges that remain. More than 800 directors responded to this year's survey, offering insight into core areas that are "top of mind" to today's world-class public companies.

BoardroomDirect

Our e-newsletter, *BoardroomDirect*, delivers our board-level developments and latest board-level insights on a monthly basis. The latest issue covers the relationship between the board and CIO regarding IT oversight, PwC's Our focus on audit quality report, the latest SEC whistleblower data, and the SEC's leadership change.

Download the Board Center App for your iPad

PwC's Board Center App provides the latest updates on corporate governance issues and trends to enable board members to more effectively meet the challenges of their critical role. The Board Center App brings together insights on strategy and growth, executive compensation, financial reporting developments, and risk management with the corporate director in mind.

For these and other PwC corporate governance publications, visit the Center for Board Governance at http://www.pwc.com/us/centerforboardgovernance.