the Corporate Governance advisor

May/June 2015 • Volume 23, Number 3

CYBERSECURITY

# Board Tools for Oversight of Cybersecurity Risk

*By Stewart M. Landefeld, Luis R. Mejia, and Allison C. Handy*

Cyber attacks on US public companies have damaged business operations, compromised corporate intellectual property and the private data of consumers, and threatened national security.[1] These attacks increased in 2014, culminating with North Korea's attack on Sony Pictures Entertainment. As a result, boards cite cybersecurity as their number one risk-related concern.[2] In exercising a board's duty of oversight, the magnitude and complexity of cybersecurity risk present special challenges.

In this article, we present the cybersecurity risks that many public company boards will consider, from the business impact of a cyber attack to the litigation and regulatory exposure that may follow. We address the oversight duty of the board and propose a methodology for fulfilling that duty. In this context, the methodology is based on the board's role of oversight as opposed to the day-to-day responsibility that

*Continued on page 2*

*Stewart M. Landefeld and Luis R. Mejia are partners, and Allison C. Handy is an associate, of Perkins Coie LLP.* *Katherine A. VanYe, Esq., provided invaluable research and writing assistance. The authors gratefully acknowledge the review and contributions of Evelyn Cruz Sroufe, Esq., John A. Seethoff, Esq., John C. Sullivan, Esq., Jeffrey A. Christianson, Esq., and Sally Barian Yates, Esq.*

Wolters Kluwer

## CONTENTS

rests with management. A board, by exercising the duty of oversight to ask the right questions and satisfy itself that appropriate internal controls are in place, can help to see that controls are in place and set an appropriate tone at the top with respect to cybersecurity matters.[3]

## Framing the Problem: Why Cybersecurity Attracts Particular Board Oversight Attention in 2015

### Impact on the Business

Incidents of large-scale cybersecurity incursion and theft picked up pace in late 2013 and grew throughout 2014 and into 2015. Two notable retailer breaches were attacks on Target in late 2013 and Home Depot in 2014. Other incursions include those on JP Morgan, the theft of US Postal Service employee data, the breach of health insurers Anthem's and Premera Blue Cross's customer data, including Social Security numbers, and North Korea's attack on Sony.

The Target incursion reported in December 2013 compromised the records of as many as 70 million customers[4] and resulted in $145 million in data breach-related expenses.[5] Although CEO and Board Chair Gregg Steinhafel, a 35-year Target veteran, took a proactive role, Target announced his resignation in May 2014, linking it to the data breach.[6]

On September 18, 2014, Home Depot, North America's largest home improvement retailer, confirmed that its payment data system had been breached.[7] Home Depot noted that the breach would impact customers in the United States and Canada who had used payment cards between April and September 2014—a five-month period—putting up to 56 million credit and debit cards at risk. Home Depot, following lessons from Target, immediately pledged to provide free credit monitoring and other identity-protection services and to cover customer liabilities for fraudulent claims. The company explained that it had taken months over the course of 2014 for its cybersecurity team to understand the magnitude of the 2014 incursions—during a time that Home Depot was completing a major encryption improvement project.[8] The company estimated that costs related to the breach could total $62 million (offset by $27 million in insurance recoveries). Although Home Depot said that it was not able, as of September, to estimate further costs or ranges of costs related to the breach, it also warned that the impact of the data breach could have a material and adverse effect on Q4 2014 and future fiscal periods.

### Litigation Risk

In addition to the significant time, resources, and capital expenditures required to respond to a cybersecurity breach, there is the risk of litigation and regulatory scrutiny. For example, Target recently settled a consumer class action related to its data breach for $10 million.[9] Target also is the subject of a class action by issuer banks whose customers' data was stolen.[10] Litigation also has resulted from cybersecurity breaches at other companies, including Sony, St. Joseph Services Corporation, Zappos, LinkedIn, and SAIC.[11] Although some of the cases have been dismissed or settled, the companies have incurred substantial legal fees and the litigation has been a distraction to normal operations.

### Regulatory Risk—Federal Consumer Protection

The Federal Trade Commission (FTC) enforces federal statutes and regulations that impose data security requirements on companies, including the Safeguards Rule (which implements the Gramm-Leach-Bliley Act),[12] the Fair Credit Reporting Act,[13] and the Children's Online Privacy Protection Act.[14] These acts and regulations govern data security requirements and disclosure and disposal of consumer information. The Federal Trade Commission Act's prohibition against unfair or deceptive acts or practices also has been used by the FTC in cases of false or misleading claims about a company's data security procedures, or failure to employ reasonable security measures that result

in substantial consumer injury.[15] According to Jessica Rich, the director of the Bureau of Consumer Protection at the FTC, the FTC has brought such cases when a company's practices as a whole demonstrated "multiple and systemic" failures.[16] In congressional testimony, she noted that "the [FTC] has made clear that it does not require perfect security; that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law."[17]

In early 2015, President Obama called for federal legislation—the "Personal Data Notification & Protection Act"—to mandate a single, national standard requiring companies to inform their customers within 30 days of discovering that their data has been hacked. The President has suggested this as a replacement to the many less-than-uniform state disclosure laws.[18]

For telecommunications and other businesses in the communications industry, a committee tasked by the Federal Communications Commission (FCC) to give advice on implementation of cybersecurity risk management has focused on communications businesses as part of the national critical infrastructure. In March 2015, the committee issued a Cybersecurity Risk Management and Best Practices Final Report.[19] The FCC Final Report's goal was to provide cybersecurity best practices for the communications industry to assist with implementation on a voluntary basis of the "NIST Framework" (The National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*),[20] developed pursuant to the President's February 12, 2013, Executive Order No. 13636, Improving Critical Infrastructure Cybersecurity. The FCC Final Report identifies voluntary mechanisms to provide assurances that FCC-regulated companies are addressing cybersecurity risks, including voluntary meetings with the FCC and the Department of Homeland Security (DHS), and participating in a DHS program on integrating and coordinating critical infrastructure cross-sector efforts.

## Regulatory Risk—The SEC's Interest in Cybersecurity

The Securities and Exchange Commission (SEC) has shown interest in cybersecurity, but to date has not brought an enforcement action against a public company related to cybersecurity. Enforcement activity has been limited to registered broker-dealers and investment advisors, that is, entities that are subject to specific regulations governing the security and confidentiality of customer records and information.[21]

In October 2011, the SEC's Division of Corporation Finance provided guidance on disclosure obligations relating to cybersecurity risks and cyber incidents, stating that the existing disclosure structure under SEC regulations provides for both timely and sufficient disclosure of material cybersecurity attacks, risks and events. Existing disclosure requirements have at least six areas in which disclosure in periodic reports on Forms 10-K and 10-Q (and certain other disclosure documents) may call for cybersecurity disclosure.[22] The SEC's 2011 guidance stresses that only material information need be disclosed; however, the SEC's actions have been somewhat inconsistent with its guidance. In several comment letters, the SEC has pushed for disclosure of all cybersecurity events, regardless of materiality.[23] Boards should anticipate some dialogue between the company and the SEC on this issue in the event of a cyber attack.

Examples of recent disclosures of cybersecurity risks in the six areas identified in the 2011 guidance include:

- *Risk Factors*. The 2011 guidance specifically called out Risk Factors as appropriate for disclosure of material cybersecurity risks and this section is currently the most frequent home for such disclosures. For example, Target discussed specific risk factors related to its data breach, and candidly stated that it might not be able to prevent future breaches given that the techniques for attacks change frequently and are difficult to detect.[24]

- *MD&A*. Cybersecurity risk could constitute a classic "trend" or "material event,

trend or uncertainty reasonably likely to have a material impact on the organization's operations, liquidity, or financial condition" that would be required to be discussed in Management's Discussion and Analysis of Financial Condition and Results of Operation (MD&A). Home Depot, for example, in its first Form 10-Q after its data breach, included an extensive discussion of the breach in its MD&A. This disclosure included discussions of the expenses incurred, litigation, claims, and government investigations, future costs, and insurance coverage.[25]

- *Description of Business*. If cybersecurity risks materially affect products, services, relationships with customers or suppliers, or competitive conditions, a registrant should disclose the cybersecurity risks in the Description of Business section. Target, in its first Form 10-K after the data breach, highlighted the breach with a brief description and cross reference to its MD&A discussion.[26]

- *Legal Proceedings*. Data breaches or cybersecurity incidents can result in material regulatory investigations or private actions that will require discussion in the Legal Proceedings section. Both Target and Home Depot, in the Forms 10-Q and 10-K that each company filed after their respective data breaches, incorporated by reference the legal proceedings discussion from the MD&A in the Legal Proceedings section.[27] In the case of Target, this cross-reference was included despite the company's assessment that these legal proceedings did not rise to the level of materiality generally required for disclosure in the Legal Proceedings section.

- *Financial Statement Disclosures*. When the risks or damages have a material financial impact on the registrant, cybersecurity risks and incidents that represent substantial costs in prevention or response should be included in financial statement disclosures. Target, for example, has updated its financial statement disclosures each quarter to quantify expenses incurred due to the data breach.

- *Disclosure Controls and Procedures*. If a cybersecurity incident impairs a registrant's ability to record or report information that must be disclosed, it may impact Disclosure Controls and Procedures. (The authors have not yet seen an example of a discussion of a failure or weakness in disclosure control and procedures caused by a cybersecurity incident.)

*Current Report on Form 8-K.* In addition to these areas that the SEC highlighted in periodic reports, a registrant might also determine that it needs to file a current report on Form 8-K in connection with a cybersecurity incident. Some companies that have complied with the state-mandated consumer notification laws mentioned previously also have determined that the breach rises to the level of materiality of a report on Form 8-K. For example, in August 2014, Community Health Systems filed a Form 8-K to disclose a data breach affecting 4.5 million customers.[28] The compromised data included patient names, addresses, birthdates, telephone numbers, and Social Security numbers.[29] Unlike Community Health Systems, however, Anthem did not file a Form 8-K in connection with its February 5, 2015 notification to its members of a cyber attack that resulted in exposure and theft of up to 80 million records, including Social Security numbers. (Anthem did include discussion of the data breach in its Form 10-K filed February 24, 2015.)

## Board and Committee Oversight of Risk and Cybersecurity

### Board Oversight of Risk

A board's responsibility to oversee cybersecurity risks arises from the "duty of oversight" developed under Delaware law. Oversight grows out of what Delaware courts consider the fundamental fiduciary obligations of directors: the duties of care and of loyalty.[30] Since the 1996 Delaware Court of Chancery decision, *In re Caremark International Inc. Derivative Litigation*,[31] directors have understood that they do not fulfill their oversight duties by passively receiving information from management.

Instead, boards must assure themselves that information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance.[32]

The *Caremark* court postulated that a board could potentially be liable for violations of law by the corporation, even if the directors had no knowledge, or even grounds for suspicion of the wrongdoing, if its failure to establish systems designed to detect such violations amounted to bad faith.[33]

In 2006, a decade after *Caremark*, the Delaware Supreme Court, in *Stone v. Ritter*, clarified when the *Caremark* framework will result in director oversight liability. When a claim of director liability is based on *ignorance* of corporate wrongdoing, "only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists—will establish the lack of good faith that is a necessary condition to liability."[34]

Litigation and SEC enforcement actions springing from the financial crisis of 2008 have further explored the board oversight responsibility described in S*tone* in 2006. For example, when may a board be liable for failure to monitor business risk that did not involve corporate wrongdoing?[35] In *In re Citigroup Inc. Shareholder Derivative Litigation*, the Delaware Court of Chancery rejected claims of personal liability against the Citigroup board for failure to monitor and address the risks posed by the bank's exposure to the subprime mortgage market, stating: "Oversight duties under Delaware law are not designed to subject directors, even expert directors, to *personal liability* for failure to predict the future and to properly evaluate business risk."[36] Despite this forceful Delaware statement in support of directors who exercise their oversight duties in good faith, plaintiffs have begun more recently to bring claims against boards for failure of oversight in some of the major cyber attacks of later 2013–2014.[37]

Wyndham Worldwide Corporation's board provided an illustration of a board satisfying its oversight obligations. The district court described the board's actions surrounding Wyndham data breaches in *Palkon v. Holmes*.[38] A shareholder had filed a derivative action against the board and others, claiming that Wyndham's failure to implement adequate cybersecurity measures and to disclose the data breaches in a timely manner caused damage to shareholders. The shareholder also alleged that the board wrongfully refused to sue the company's officers. The *Palkon* court found that the board's refusal to pursue litigation was a good-faith exercise of business judgment, made after a reasonable investigation. Although the court did not reach the merits of the underlying claim, it noted that the plaintiff conceded that security measures existed when the first breach occurred, and that the board had repeatedly addressed security concerns. The full board had discussed the cyber attacks, the company's security policies, and proposed security enhancements at 14 meetings over a four-year period, and the audit committee had addressed the same issues in at least 16 committee meetings during the same time period. The company had hired technology firms to investigate each breach and to issue recommendations on enhancing the company's security, and it followed those recommendations. Under these circumstances, the court, following *Caremark* and *Stone*, found that it would have been difficult for the plaintiff to establish that the board "utterly failed to implement any reporting or information system … [or] consciously failed to monitor or oversee its operations thus disabling themselves from being informed."[39]

In addition to the state law duty of oversight, companies have sharpened their focus on board oversight of risk in light of the disclosure requirement under SEC Regulation S-K Item 407(h), which was added in the SEC's proxy disclosure enhancements in 2009.[40] This item, which is required in proxy statements and certain other public filings, calls for disclosure of the extent of

the board's role in risk oversight. In a June 2014 speech, SEC Commissioner Luis Aguilar noted that boards' increasing focus on risk oversight must encompass oversight of cybersecurity risks.[41]

### Board and Committee Oversight of Cybersecurity

Boards exercise their risk oversight responsibilities through a variety of ways. Generally, management provides periodic briefings on significant risks that a company faces and how it seeks to control risk. Board and executive team discussions of risk occur both at regular meetings and with a specific risk analysis of new ventures at an annual strategic planning session. Often, the board exercises direct oversight of certain specific risks, and delegates oversight of other specific risks to a committee (for example, compensation plan risks to the compensation committee, financial reporting risk to the audit committee, and so on). Committees can provide effective oversight by devoting close and sustained attention in a small group—a compelling benefit when dealing with complex matters having a short time fuse. Large public company board meetings are scheduled a year or more in advance, although committees can meet with greater frequency and flexibility. Committees can be more responsive and, in small group discussion, can better take advantage of the special skills and backgrounds of committee members.

Risk committees (for financial institutions) and audit committees monitor many risks for most companies and could take on delegated oversight of cybersecurity. Boards alternatively delegate cybersecurity oversight to a regulatory affairs committee or to another committee with appropriate mandate and membership. It is rare for a company to have a cybersecurity risk committee.[42]

In delegating to a committee, both the Delaware General Corporation Law and the Model Business Corporation Act require appropriate board oversight of the committee's work. The SEC has brought enforcement actions against board members who were not diligent and attentive to matters that they had delegated to a committee.[43]

## Best Practices for the Board in Managing Cybersecurity Risk

Boards, and the assigned committee (often audit), can think of their task of overseeing cybersecurity in three stages. The methods are similar to those of overseeing other enterprisewide operational risks.

First, what is the frequency and depth with which the board or committee will review cybersecurity issues? Because cybersecurity is one of a number of important operational risks, the board, together with the CEO, chief financial officer, and general counsel, can set an appropriate frequency, such as twice-a-year presentations on cybersecurity to the assigned committee. The committee would then "report out" on the topic to the full board as a standalone report or as part of a broader report on operational risks. The full board could choose to have a detailed discussion when it conducts its annual in-depth review of enterprisewide risk issues. The board or committee also will want to address cybersecurity (and review a response plan to cyber incursions) as part of its periodic review of the company's crisis management plan.

Second, what are the resources available to the board or committee and on whom do the directors rely for their review? Generally, the first resource is senior management. Management can educate the board on cybersecurity generally, help the board to assess threats specific to the company, and explain the company's current defenses and mitigations to those threats. Usually, the appropriate person to present to the audit committee is the internal owner of cybersecurity, for example, a chief information officer. He or she can present an agenda that could include

(1) the cybersecurity environment of threats and how this environment fits into the company's overall operational risk framework;

(2) attacks on the company in the last 12 months and how they were addressed;

(3) the program for the coming year, including the structure, operation, and testing of security and privacy programs;

(4) a multiple-year program roadmap (past and forward) and budget;

(5) a comparison of the company program to the current NIST Framework or other appropriate industry standard;

(6) known trends of industry risks and efforts to enhance cybersecurity in the coming year; and

(7) emerging issues including monitoring and mitigating device (*e.g.*, smartphone or tablet) threats, and managing the risks of big data.

Some boards use a third-party consultant as an additional resource. The advisor could assist the assigned committee to understand best practices in the company's industry. Third parties can help to bring perspective, aiding directors in assessing the management team as a source other than the team itself. If a change in leadership of the cybersecurity function occurs, having a consistent third-party advisor can help the board or committee assess whether the program has maintained continuity.

## Questions for the Audit Committee to Ask the Manager of Cybersecurity Risk

Third, at the heart of any board oversight exercise are thoughtful questions from its directors. These questions, paired with management's responses over time, are the essence of oversight, and can lead to process improvements. (A general counsel can help the board develop these questions as a starting point for its inquiry.) In the same way that Warren Buffett has suggested four questions to assist an audit committee in discussions with its outside auditors,[44] the board or audit committee can pose this basic set of a half-dozen questions[45] as tools to understand and oversee the management of cybersecurity:

1. *Ownership.* Who owns the cybersecurity risk for our company? To whom does she report? Has she assessed the scale and probability of attacks or incursions, as well as the most likely areas of vulnerability (internal threats, third-party vendors) against the company?

2. *Controls.* Have we designed and implemented strong internal controls that address our cybersecurity risks and ensured that our internal controls are well documented, communicated, and updated as needed? Have our controls identified attempted or successful cybersecurity breaches or attacks?

3. *NIST Framework.* Does the company use the NIST Framework or, if not, what other appropriate framework is used? How do our framework and controls compare with those of others in our industry?

4. *Budget.* Does the company have the appropriate budget to manage the cybersecurity function and develop a satisfactory team? Are there needs that have not been met due to budget? Does the company use a third party for a security audit?

5. *Crisis Response.* Do we have an incident response plan in place? Does the plan include all the relevant stakeholders as owners with specific responsibilities? Does the plan incorporate what we have learned from attacks against us and our competitors? Are we prepared to respond to legal, reputational, and commercial risks and obligations? Are we satisfied with our insurance coverage?

6. *Disclosure*. Does the company have a form of consumer notice and Form 8-K prepared for an incursion? Does the company provide an investor reading our Form 10-K a clear picture of our risk profile and how our company's operations impact our cybersecurity risk profile?

## Conclusion

Cybersecurity will continue to evolve as a risk and will demand increasing oversight by boards of public companies. Boards have

available to them the tools required to oversee this key operational risk. A successful plan for oversight will be to first determine the scope of board review and then to establish the resources available to the board in making its inquiries. Developing key questions for management, and responding thoughtfully to such questions, are at the heart of this oversight process. Finally, applying this process over time will allow the board to see how cybersecurity threats to the company evolve with the company's changing business. A board using these tools effectively can become as confident as reasonably practical that the company is taking appropriate steps to address the evolving cybersecurity risk.

## Notes

1. *See* Press Release, Hewlett-Packard Dev. Co., "HP Reveals Cost of Cybercrime Escalates 78 Percent, Time to Resolve Attacks More Than Doubles" (Oct. 8, 2013), *http://www8.hp.com/us/en/hp-news/press-release.html?id=1501128*, last accessed March 29, 2015 (study by Ponemon Institute sponsored by Hewlett-Packard, that by 2013 the average annualized cost of cybercrime to a sample of US companies was $11.6 million per year, representing a 78 percent increase since 2009).

2. FTI Consulting Inc. & NYSE Governance Servs., *Law in the Boardroom in 2014* (May 19, 2014), *http://www.fticonsulting.com/global2/media/collateral/united-states/law-in-the-boardroom-in-2014.pdf*, last accessed March 29, 2015.

3. Cybersecurity is a contingent risk, that is, one whose impact on a business is uncertain, because it is contingent on future outcomes. More than many other contingencies that may hinge on one or two events, cybersecurity repays board attention over time, as cybersecurity-related threats will adapt to changes in the business itself. *See* Gregory F. Treverton, "Risks and Riddles," *Smithsonian Mag*., June 2007, available at *http://www.smithsonianmag.com/people-places/risks-and-riddles-154744750/*, last accessed March 29, 2015 (discussion of complex contingencies).

4. Target Corp., Annual Report (Form 10-K) (Mar. 14, 2014).

5. Target Corp., Annual Report (Form 10-K) (Mar. 13, 2015).

6. Press Release, Target Corp., Statement from Target's Board of Directors (May 5, 2014), *http://pressroom.target.com/news/statement-from-targets-board-of-directors*, last accessed March 29, 2015.

7. Press Release, The Home Depot, Inc., "The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores" (Sept. 18, 2014), *http://media.corporate-ir.net/media_files/IROL/63/63646/HD_Data_Update_II_9-18-14.pdf*, last accessed March 29, 2015.

8. *See* Nicole Perlroth, "Home Depot Says Data From 56 Million Cards Was Taken in Breach," *N. Y. Times*, Sept. 18, 2014, available at *http://bits.blogs.nytimes.com/2014/09/18/home-depot-says-data-from-56-million-cards-taken-in-breach/?_r=0*, last accessed March 29, 2015.

9. *See* George Stahl, "Target to Pay $10 Million in Class Action Over Data Breach," *Wall Street J.*, Mar. 19, 2015, *available at http://www.wsj.com/articles/target-to-pay-10-million-in-class-action-over-data-breach-1426768681?mod=rss_Technology*, last accessed March 29, 2015.

10. *See In re Target Corp. Customer Data Sec. Breach Litig*., MDL No. 14-2522 (D. Minn. Dec 2. 2014).

11. *See, e.g., In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014); *In re LinkedIn User Privacy Litig.*, No. 5:12-CV-03088-EJD, 2014 WL 1323713 (N.D. Cal. Mar. 28, 2014).

12. 16 C.F.R. pt. 314, implementing 15 U.S.C. § 6801(b).

13. 15 U.S.C. § 1681. The FTC's implementing rule is at 16 C.F.R., pt. 682.

14. 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. pt. 312.

15. *See Discussion Draft of H.R. __, Data Security and Breach Notification Act of 2015 Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. on Energy and Commerce*, 114th Congress 3 n.8 (2014) (statement of Jessica Rich, Director, Bur. of Consumer Prot., Fed. Trade Comm'n) available at *https://www.ftc.gov/system/files/documents/public_statements/630961/150318datasecurity.pdf*, last accessed March 29, 2015 ("If a company makes materially misleading statements or omissions about a matter, including data security, and such statements or omissions are likely to mislead reasonable consumers, they can be found to be deceptive in violation of Section 5 [15 U.S.C. § 45]. Further, if a company's data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and violate Section 5.").

16. *Id.* at 3.

17. *Id.*

18. Michael D. Shear and Natasha Singer, "Obama to Call for Laws Covering Data Hacking and Student Privacy," *N.Y. Times*, Jan. 11, 2015, available at *http://www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html?_r=0*, last accessed March 29, 2015.

19. Commc'ns Sec., Reliability and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report* (Mar. 18, 2015), *http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf*, last accessed March 29, 2015.

20. Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*, last accessed March 29, 2015.

21. The SEC's attention to controls of regulated broker-dealers and investment advisors may be a predicate to future SEC staff focus on the importance of cybersecurity to internal controls, for nonfinancial institution registrants. *See* Deloitte, *The SEC's Focus on Cybersecurity: Key Insights for Investment Advisers* (Sept. 2014), available at *http://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-the-secs-focus-on-cyber-security-070914.pdf*, last accessed March 29, 2015; SEC, Cybersecurity Roundtable (Mar. 26, 2014), available at *http://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt*, last accessed March 29, 2015.

22. Div. of Corp. Finance, SEC, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011), available at *https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm*, last accessed March 29, 2015.

23. *See*, *e.g.*, *Comcast Corp.* SEC Comment Letter (June 28, 2012); *Honeywell Int'l Inc.* SEC Comment Letter (May 17, 2012).

24. Target Corp., Annual Report, *supra* note 4.

25. The Home Depot, Inc., Quarterly Report (Form 10-Q) (Nov. 25, 2014).

26. Target Corp., Annual Report, *supra* n.4.

27. *See id.*; Home Depot, Quarterly Report *supra* n.25.

28. Community Health Systems, Inc., Current Report (Form 8-K) (Aug. 18, 2014).

29. *Id.*

30. *See Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362 (Del. 2006); *see also Mills Acquisition Co. v. Macmillan, Inc.,* 559 A.2d 1261 (Del. 1989); *Aronson v. Lewis*, 473 A.2d 805 (Del. 1984), *overruled in part by Brehm v. Eisner*, 746 A.2d 244 (Del. 2000). Similarly, the Model Business Corporation Act § 8.30(b) (3d ed. 2003) provides that board members "shall discharge their duties with the care that a person in a like position would reasonably believe appropriate under similar circumstances."

31. 698 A.2d 959 (Del. Ch. 1996).

32. *Id.* at 970.

33. *Id*. at 971.

34. *Stone*, 911 A.2d at 364 (quoting *Caremark*, 698 A.2d at 971).

35. *See In re Citigroup Inc. Shareholder Derivative Litig.*, 964 A.2d 106 (Del. Ch. 2009); *In re The Goldman Sachs Group, Inc. Shareholder Litig.*, C.A. No. 5215-VCG (Del. Ch. 2011). *See generally* Luis A. Aguilar, Comm'r, Sec. & Exchange Comm'n, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Speech Before the New York Stock Exchange (June 10, 2014), *http://www.sec.gov/News/Speech/Detail/Speech/1370542057946*, last accessed March 29, 2015.

36. 964 A.2d at 131.

37. *See In re Target Corp. Customer Data Sec. Breach Litig.,* MDL No. 14-2522 (D. Minn. Dec 2. 2014); *Palkon v. Holmes,* No. 2:14-CV-01234 (SRC), 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

38. 2014 WL 5341880.

39. *Id.* at *6 n. 1.

40. *See* Proxy Disclosure Enhancements, SEC Release No. 33-9089 (Dec. 16, 2009), 74 Fed. Reg. 68,334 (Dec. 23, 2009), available at *http://www.sec.gov/rules/final/2009/33-9089.pdf*, last accessed March 29, 2015.

41. Aguilar, *supra* n.35.

42. Deloitte, *Risk Intelligent Proxy Disclosures — 2013: Trending upward* (2014), *http://deloitte.wsj.com/riskandcompliance/files/2014/01/Risk_Intelligent_Proxy_Disclosures_2013.pdf*, last accessed March 29, 2015.

43. *Alderman*, Investment Company Act Release No. 30300, AP File No. 3-15127 (Dec. 10, 2012).

44. Warren Buffet, Annual Letter to Shareholders of Berkshire Hathaway Inc. (Feb. 21, 2003), available at *www.berkshirehathaway.com/letters/2002pdf.pdf*, last accessed March 29, 2015.

45. *See* Paul A. Ferrillo, Dave Burg and Aaron Philipp, "The Cloud, Cybersecurity, And Cloud Cyber Governance: What Every Director Needs To Know," Metropolitan Corp. Counsel, Aug. 13, 2014, available at *http://www.metrocorpcounsel.com/articles/29549/cloud-cybersecurity-and-cloud-cyber-governance-what-every-director-needs-know*, last accessed March 29, 2015, for helpful cloud-specific questions.

# Is Employee Awareness and Training the Holy Grail of Cybersecurity?

***By Paul Ferrillo and Randi Singer***

They may be based in North Korea, Russia, China, or the United States. They may call themselves "Deep Panda," "Axiom," "Group 72," the "Shell_Crew," the "Guardians of Peace," or the "Syrian Electronic Army." But no matter how exotic or mundane the origins of a particular cyber-criminal organization, all that it needs to initiate a major cyberattack is to entice one of your employees to click on a malicious link in an email, inadvertently disseminate malware throughout the network servers, and potentially cause tremendous damage and loss of business.[1]

Indeed, "spear phishing" is a tactic used by cyber-criminals that involves sending phony, but seemingly legitimate, emails to specific individuals, company divisions, or even business executives, among other unwitting targets. Unlike spam, these emails usually appear to be from someone the recipient knows and in many cases can appear completely legitimate, or at least unassuming. If the recipient opens any attachments or clicks any links, havoc can ensue. Such spear phishing emails are suspected to have caused many of the recent major cyber attacks. Despite fancy-sounding defensive cybersecurity devices at companies and financial institutions, "spear phishing with malware attachments" is often the easiest route into a sophisticated network.[2]

One report recently noted that,

> Compared to the "spam-phishing" emails of days past, which most people have learned to identify and avoid over the years, spear-phishing emails are astronomically more effective. Whereas the current open rate for spam emails is a meager 3%, the open rate for spear-phishing emails is a staggering 70% (not to mention 50% of those who open these emails also click the links they contain). A study published by Cisco found 1,000 spear-phishing emails generate ten times more data revenue for hackers than sending 1,000,000 spam-phishing emails.[3]

According to another recent study, 90 percent of all hacks in the first half of 2014 were preventable, and more than 25 percent were caused by employees.[4]

For these reasons, it is absolutely crucial that a company provide training to its employees to detect and avoid spear-phishing attacks, and more broadly, avoid common lapses in judgment



the Corporate Governance Advisor

Copyright © 2015 CCH Incorporated. All Rights Reserved.

The ***CORPORATE GOVERNANCE ADVISOR*** (ISSN 1067-6171) is published bimonthly by Wolters Kluwer at 76 Ninth Avenue, New York, NY 10011. Subscription rate, $775 for one year. POSTMASTER: Send address changes to *THE CORPORATE GOVERNANCE ADVISOR,* Wolters Kluwer, 7201 McKinney Circle, Frederick, MD 21704. Send editorial correspondence to Wolters Kluwer, 76 Ninth Avenue, New York, NY 10011. To subscribe, call 1-800-638-8437. For Customer service, call 1-800-234-1660. This material may not be used, published, broadcast, rewritten, copied, redistributed or used to create any derivative works without prior written permission from the publisher.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other professional assistance is required, the services of a competent professional person should be sought.

—From a Declaration of Principles jointly adopted by a committee of the American Bar Association and a Committee of Publishers and Associations.

**Permission requests:** For information on how to obtain permission to reproduce content, please go to *http://www.wklawbusiness.com/footer-pages/permissions.*

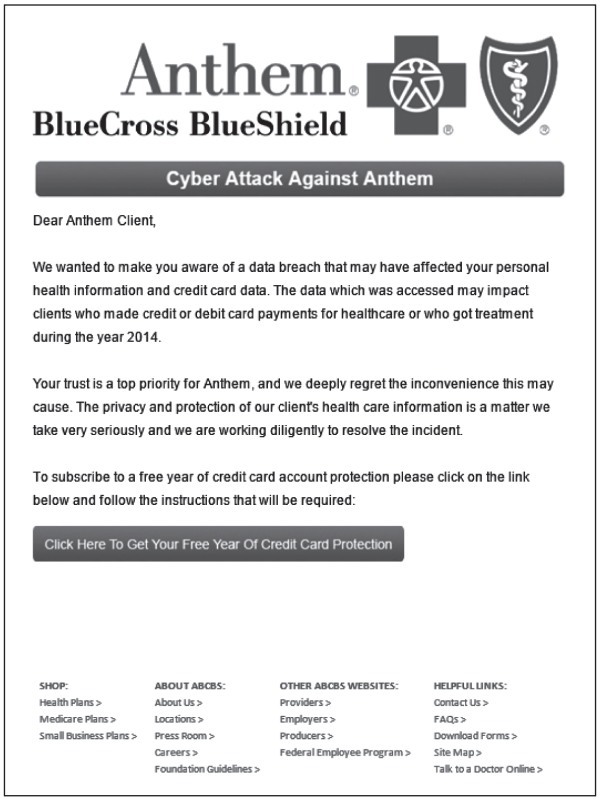
**Purchasing reprints:** For customized article reprints, please contact *Wright's Media* at 1-877-652-5295 or go to the *Wright's Media* website *www.wrightsmedia.com.*

**www.wklawbusiness.com**

or awareness that can expose a company to a cyber-incident. For example, companies can easily offer training that improves password protection, helps avoid workplace theft, and better protects employee-owned devices without password protection such as smartphones, laptops, and tablets. Though no one particular training regimen can provide guaranteed protection from a cyber-attack, statistics support their inclusion as a critical part of a company's overall security posture.

## Anti-Spear-Phishing Training

Weeks after the announcement of the Anthem attack, which, like that on Sony Pictures, was likely caused by a sophisticated spear-phishing operation, cybersecurity guru Brian Krebs noted that others were attempting to prey upon the misfortune of more than 80 million patients by sending their own spoofed emails to affected customers.[5] Other "cold-calling" scams apparently were perpetrated at about the same time as the fake emails were sent:



Anthem®
BlueCross BlueShield®

**Cyber Attack Against Anthem**

Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. The privacy and protection of our client's health care information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required:

Click Here To Get Your Free Year Of Credit Card Protection

| SHOP: | ABOUT ABCBS: | OTHER ABCBS WEBSITES: | HELPFUL LINKS: |
|---|---|---|---|
| Health Plans > | About Us > | Providers > | Contact Us > |
| Medicare Plans > | Locations > | Employers > | FAQs > |
| Small Business Plans > | Press Room > | Producers > | Download Forms > |
| | Careers > | Federal Employee Program > | Site Map > |
| | Foundation Guidelines > | | Talk to a Doctor Online > |

Now, if you were a terrified Anthem patient whose personal health information was potentially stolen, this sort of an email communication would not be unexpected, and would be very appealing; it would be natural to click the link. In reality, clicking on the fraudulent "free credit protection link" would only have touched off a whole new world of pain.

Here is another example illustrating the growing sophistication of spear-phishing attacks. What if you were an existing customer of HSBC and received this email? Would you click on the link, or ignore it and potentially let your account be suspended by "the bank"?[6]

HSBC

HSBC Bank plc

Customer ID : 000-5432-654386-PSI

Dear Valued HSBC Customer

This e-mail is to inform you that your account will be suspended within 48 hours due to your Account Inactivity. You will have to confirm certain Account Information in order to continue your account subscription :

https://Securityalert.HSBC.co.uk/1/2/

HSBC Bank Plc
Security Advisor
HSBC Bank PLC.

Please do not reply to this e-mail. Mail sent to this address cannot be answered.
For assistance, log in to your HSBC Online Bank account and choose the "Help" link on any page.

HSBC Email ID # 1009

But the potential price for opening a link that does not appear to be obviously suspicious can be breathtakingly high. In an era in which there is so much personal information about everyone on the Internet, it would not be hard for even a high-school student to create an authentic-looking email that could catch us when we least suspect a cyberattack (especially the Anthem "customer email"). Even higher-level employees are vulnerable to spear phishing (often called "whaling" when high-level executives are targeted), and the corresponding damage can be exponentially worse.[7]

How do you guard against a socially engineered spear-phishing attack? You train and you train, and then you train some more. Many corporate IT departments already periodically send out fake emails to their employees hoping

for a "bite." Many more companies regularly train their employees monthly on anti-spear-phishing using automated computer programs that send emails to employees from exact Web site addresses to see who will unwittingly click on the links.[8] Records can be kept of successes (and failures). Some companies might award prizes to employees who religiously resist getting tricked, gaining loyalty while simultaneously lowering risk. Lowering the risks of an employee clicking on a malware-infected spear-phishing email can be substantial.[9]

## Password Protection and Awareness

There also has been a tremendous amount of publicity over the inadequacy of employee passwords. A January 2013 report by Deloitte suggests that an astonishing 90 percent of user passwords are vulnerable to hacking.[10] There are a few rules of the road:

1. Companies should force employees to change their passwords regularly (preferably every 30 days), without exception;

2. Employee passwords cannot be common defaults such as "password" or "12345";[11]

3. Employees should not store passwords on sticky notes placed on their computers or in a physical or digital file or folder called "password";

4. Employee passwords should be strong; rather than the first name of the employee's child, dog or cat, it should contain unique patterns of letters, numbers and other signs, like "I li6e cho$hlat@";

5. Employees should be required to install passwords on any device used to access company email or any company resources, including home laptops, so that they remain secure as well;

6. Companies should make sure that employees follow responsible "social media" practices with regard to company-specific information;

7. Companies should provide privacy screens to employees to prevent "shoulder surfing" (reading over an employee's shoulder); and

8. Employees should receive frequent training on spear phishing, so no employee inadvertently gives up his password to an unauthorized third party.

## Other Simple (Non-Hardware) Ideas to Protect Company Data

Finally, for any company, it is important for the IT department to reinforce the following best practices for the handling of company data:

1. Follow least-access principles and control against over-privileging. An employee should only be given access to the specific resources required to do his or her job. Not every employee needs the keys to the kingdom.

2. Make sure software patches and critical updates are made in a prompt and timely fashion so that no critical patch is left uninstalled for lack of time or budget.

3. Every company should instill within each employee a sense of "ownership" in the collective good of the company, one that requires him or her to be cyber-conscious and sensitive to the potential areas of susceptibility described previously.

Cybersecurity is the ultimate team sport, and every person in the company, from a director down to an entry-level employee, needs to be invested in its cybersecurity:

> The infamous Sony hack, the systematic attacks of Heartbleed and Shellshock targeting core internet services and technologies, and the new wave of mass mobile threats have placed the topic of security center stage. Organizations are dramatically increasing their IT budgets to ward off attack but will continue to be vulnerable if they over-invest in technology while

failing to engage their workforce as part of their overarching security solution. If we change this paradigm and make our workforce an accountable part of the security solution, we will dramatically improve the defensibility of our organizations.[12]

We cannot claim that any of these ideas are cure-alls for the hacking problem in the United States (in fact, none are complete solutions). We can only subscribe to the theory that failing to implement basic cybersecurity "blocking and tackling" practices is the functional equivalent of forgetting to lock the back door.

## Notes

1. *See* "Learning from the Mistakes of Others: Sony, NSA, G2O, & DoD Hacks," available at *http://www.nextech.com/blog/learning-from-the-mistakes-of-others-sony-nsa-g2o-dod-hacks*, last accessed March 25, 2015; *also see, e.g.* "Data Breach at Health Insurer Anthem Could Impact Millions," available at *http://krebsonsecurity.com/2015/02/data-breach-at-health-insurer-anthem-could-impact-millions/comment-page-1/*, last accessed March 25, 2015.

2. *See* "'Spear Phishing' Attacks Infiltrate Banks' Networks," available at *http://ww2.cfo.com/cyber-security-technology/2015/02/spearfishing-attacks-infiltrate-banks-networks/*, last accessed March 25, 2015.

3. *See supra* n.1.

4. *See* "Over 90 percent of data breaches in first half of 2014 were preventable," available at *http://www.zdnet.com/article/over-90-percent-of-data-breaches-in-first-half-2014-were-preventable/*, last accessed March 25, 2015; *see also* "The Weakest Link Is Your Strongest Security Asset," available at *http://blogs.wsj.com/cio/2015/02/26/the-weakest-link-is-your-strongest-security-asset/*, last accessed March 25, 2015 (noting, "According to PwC, employees and corporate partners are responsible for 60% of data breaches. Verizon's research suggests the number is even higher, at almost 80%.").

5. *See* "Phishers Pounce on Anthem," available at *http://krebsonsecurity.com/2015/02/phishers-pounce-on-anthem-breach/*, last accessed March 25, 2015.

6. *See http://cdn2-b.examiner.com/sites/default/files/styles/image_content_width/hash/4a/15/4a15ec9a368f3132c0d093d53823f1f2.jpg?itok=d1TgG9gB*, last accessed March 25, 2015.

7. *See* "Hacking the Street, FIN4 Likely Playing the Market," available at *http://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf*, last accessed March 25, 2015.

8. *See e.g.* the anti-spear phishing training offered by a company called Phishme, available at *http://phishme.com/the-phishme-advantage/roi/*, last accessed March 25, 2015.

9. *See* "KnowBe4 Security Awareness Training Blog: Train Employees And Cut Cyber Risks Up To 70 Percent," available at *http://blog.knowbe4.com/train-employees-and-cut-cyber-risks-up-to-70-percent*, last accessed March 25, 2015.

10. *See* "90 percent of passwords vulnerable to hacking," available at *http://www.businessinsider.com/90-percent-of-passwords-vulnerable-to-hacking-2013-1*, last accessed March 25, 2015.

11. *See* "This List Of 2014's Worst Passwords, Including '123456,' Is Embarrassing," *http://techcrunch.com/2015/01/20/this-list-of-2014s-worst-passwords-including-123456-is-embarrassing/*, last accessed March 25, 2015.

12. *See* "The Weakest Link Is Your Strongest Security Asset," available R *http://blogs.wsj.com/cio/2015/02/26/the-weakest-link-is-your-strongest-security-asset/*, last accessed March 25, 2015.

# Stock Ownership Guidelines & Retention Policies: Creating Stronger Links Between Executives and Shareholders

***By Jessica Yu***

Companies have used stock ownership guidelines to encourage and build stock ownership by their executives for decades. The theory, of course, is that owning company stock helps align executives' financial interests with those of shareholders.

It used to be that the standard guidelines called for CEOs to hold shares equal in value to at least five times salary, with multiples cascading downward for executives below the CEO level. Companies provided mechanisms to help executives reach their guidelines, including increasing long-term incentive grants, liberal counting of shares and derivatives, and a relatively generous time period in which to achieve compliance. Increasingly, however, companies are revising their ownership guidelines to once again set themselves apart from the pack. In other words, stock ownership guidelines have become so ubiquitous that more rigorous guidelines are increasingly required to create a meaningful link between shareholder and executive interests that stands apart from competitors and peers.

The Towers Watson Executive Compensation Resources (ECR) team's review of stock ownership guidelines and retention policies disclosed in 2014 proxy statements reveals that the vast majority of the *Fortune* 500 companies have ownership guidelines or retention policies in place. In fact, 92 percent of *Fortune* 500 companies (a universe of 478 public companies) have either ownership guidelines or a retention policy. Ninety percent have stock ownership guidelines, while 45 percent have both stock ownership guidelines and some sort of retention policy. This represents a steady increase from 43 percent of large U.S. companies that had guidelines in place in 2004 and the 75 percent reported in 2007, the year after the Securities and Exchange Commission (SEC) required companies to disclose details of their ownership guidelines in the newly revised Compensation Discussion and Analysis section of the proxy.



## Stock Ownership Guidelines Structure

The structure of stock ownership guidelines focuses on six questions.

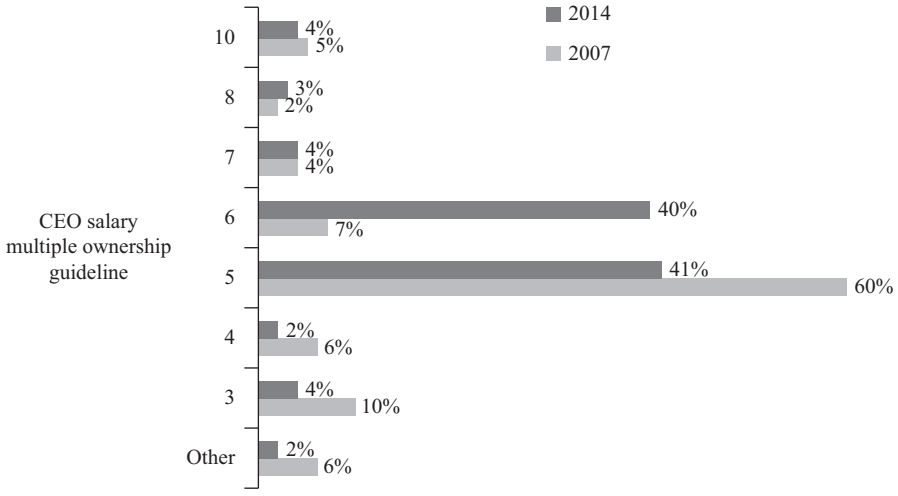
**To which executives do the guidelines apply?** Guidelines most often apply to the CEO, named executive officers (NEOs), and other high-level executives, but sometimes can be broad enough to cover hundreds of employees.

**What measures are used?** Ownership guidelines can be based on one of the following: a multiple of salary, a fixed number of shares, the lesser of a multiple of salary or a fixed number of shares, or a dollar value. The most common is multiple of salary, with 85 percent of companies using a salary multiple as their design method.

**How much must be held?** The CEO typically is expected to hold the largest multiple of stock, with other NEOs and executives required to hold declining multiples from the CEO level.

For many years, five times salary was considered the standard ownership requirement for most CEOs. However, as shown in *Figure 1,* companies are increasingly requiring CEOs to own a larger stake. Although five times salary continues to be the most common multiple applicable to CEOs (41 percent of companies), the median CEO ownership requirement has increased to six times salary as companies

**Figure 1. CEO Stock Ownership Guidelines as a Percentage of Base Salary, 2007 vs. 2014***




* Our 2007 study was based on the S&P 500 companies, the largest U.S. companies based on market capitalization. Our 2014 study focused on the *Fortune* 500, the largest U.S. companies based on revenue size. Although there's broad overlap between the two indices, comparisons should take into account the differences in the samples.

have bumped ownership requirements for CEOs upward over the past several years.

Required ownership levels for other executives have remained relatively constant over the years. CFOs, COOs, executive VPs, and division heads are typically required to hold three times salary at the median, while senior VPs are asked to hold two times salary. The typical VP ownership multiple is one time salary.

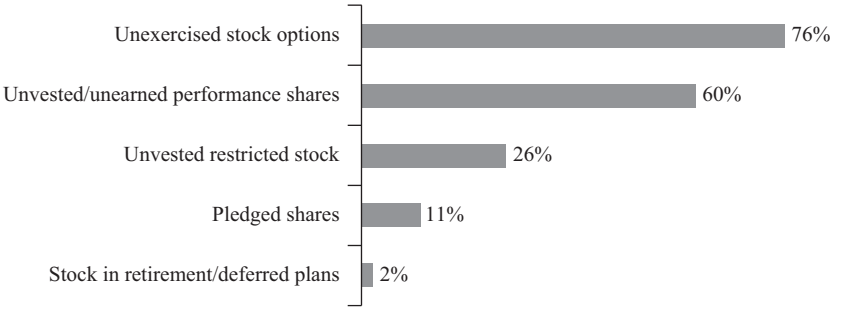
**How quickly are executives required to meet the guidelines?** An executive typically has a set number of years to accumulate the specified ownership level. More than half of all companies (54 percent) in ECR's current study provide five years for executives to meet ownership guidelines.

**How are shares valued?** Companies use a range of approaches to determine the price of shares that will apply to determine whether executives meet the guidelines. The most common way shares are valued is based on a specific date, which can be on the fiscal year end, the anniversary of the date the person was hired or on an annual grant date. Other approaches include the average of the closing prices on the final trading day of the week for the prior 52 weeks or a 200-day moving average of the stock price.

**What types of shares count toward meeting the guidelines?** Although it makes sense that shares owned outright by the executive would count toward meeting ownership requirements, companies often allow executives to count other equity when measuring compliance with guidelines. The most commonly disclosed types of share derivatives include restricted shares/restricted stock units (65 percent), retirement or deferred shares (56 percent) and shares owned by family members, partnerships, or trusts (33 percent).

Equity awards are not automatically included when determining ownership compliance. As *Figure 2* shows, the most commonly excluded equity vehicles are unexercised options and unvested performance stock (*i.e.*, awards that are not guaranteed to be earned or settled). These types of shares, as well as unvested restricted shares, have not been earned, and the value could change significantly before the executive takes ownership.

**Figure 2. Share Types Excluded in Determination of Ownership Guideline Compliance***




* Percentages are based on a subset of 362 companies from the full *Fortune* 500 sample that reported details of which types of equity are counted.

## Retention Policies Increasingly Linked to Ownership Attainment

Like ownership guidelines, retention policies are designed to link the financial interests of executives to those of shareholders. However, instead of mandating a certain level of ownership, these requirements call for executives to hold shares that are received from exercising options or from vesting equity awards for some fixed duration following exercise or settlement.

Almost half (47 percent) of *Fortune* 500 companies have retention guidelines in place, up from 24 percent when ECR reviewed these policies among the S&P 500 companies in 2007. The majority of retention policies (69 percent) require executives to retain shares only until stock ownership guidelines are met. These types of policies help ensure that executives work toward achieving their ownership targets while minimizing the importance of a defined compliance period in which to do so. An additional 10 percent of companies use a layered approach that requires executives to hold some percentage of stock proceeds until ownership guidelines are met and then hold additional shares for some longer duration.

A smaller subset of companies—21 percent of companies with retention policies—use stock retention policies on a stand-alone basis without referring to stock ownership guidelines. These policies require an executive to hold stock (usually 25 percent, 50 percent, 75 percent, or 100 percent of net proceeds) after the stock has vested for a period of time that can range from one year to after retirement. *Figure 3* shows a breakdown of typical holding periods.

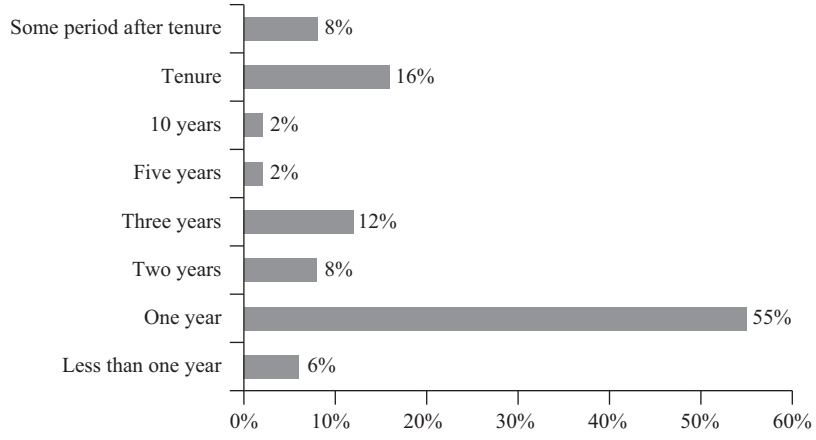
Financial services firms are more likely than other companies to have stand-alone stock retention policies. *Figure 4* shows the prevalence of ownership guidelines and retention policies by industry. Because financial firms frequently pay out incentive awards using a combination of cash and unvested stock, the retention policies essentially take the place of vesting provisions of traditional equity awards.

When we look at the *Fortune* 500 by industry, it's clear that several industries use ownership guidelines and retention guidelines more than others. Four industries have the highest percentage of companies with guidelines (100 percent):

- Food, beverage, and tobacco
- Materials
- Pharmaceuticals, biotechnology, and life sciences
- Technology hardware and equipment

Although ownership guidelines or retention policies are common among most U.S. companies, companies continue to modify

## Figure 3. Common Holding Periods for Stock Retention Policies*

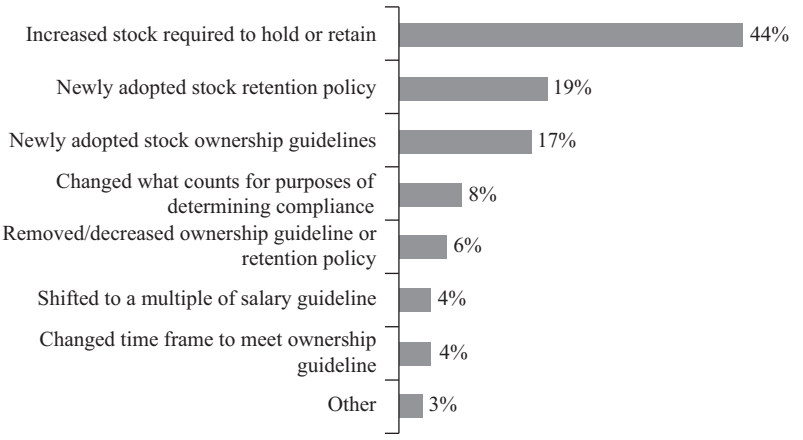



* Holding periods are classified irrespective of the proportion of stock proceeds required to be retained. Due to cases in which executives at the same company have different holding periods, the total prevalence shown is greater than 100 percent.

## Figure 4. Industry Breakdown of Guidelines and Retention Policies

| GICS Industry Group | Stock Ownership Guidelines Only | Retention Policies Only | Both Guidelines and Retention Policies | Median Multiple of Salary Ownership Guideline for CEO |
|---|---|---|---|---|
| Automobiles and components | 75% | 0% | 17% | 6 |
| Banks | 18% | 18% | 55% | 5 |
| Capital goods | 57% | 2% | 41% | 6 |
| Consumer durables and apparel | 46% | 0% | 46% | 6 |
| Consumer services | 46% | 0% | 38% | 6 |
| Diversified financials | 15% | 20% | 40% | 5 |
| Energy | 45% | 0% | 35% | 6 |
| Food and staples retailing | 47% | 0% | 47% | 6 |
| Food, beverage, and tobacco | 59% | 0% | 36% | 6 |
| Healthcare equipment and services | 35% | 0% | 61% | 5 |
| Insurance | 33% | 0% | 63% | 5 |
| Materials | 34% | 0% | 66% | 5 |
| Media | 53% | 0% | 18% | 6 |
| Pharmaceuticals, biotechnology, and life sciences | 60% | 0% | 40% | 6 |
| Retailing | 47% | 2% | 38% | 5 |
| Software and services | 47% | 0% | 47% | 6 |
| Technology hardware and equipment | 59% | 0% | 41% | 5 |
| Transportation | 61% | 0% | 39% | 5 |

**Figure 5. Common Changes Made to Stock Ownership Guidelines and Retention Policies***




* Percentages do not add to 100 percent, as some companies made more than one change to their guidelines or retention policies. "Other" includes adding time to a retention provision, removing special provisions for executives at retirement age, calculating the value of the stock differently, adding a noncompliance (penalty) clause and moving from a set time period to using the retention policy to meet guidelines.

programs as business needs change and market practices evolve. In total, 145 companies, or 30 percent of the sample, made changes to their stock ownership and retention policies during the past two years. The most common change was to increase the amount of stock that executives must hold or retain. *Figure 5* shows common changes companies made to stock ownership guidelines and retention policies in recent years.

Because companies have used stock ownership guidelines for years, and the vast majority of *Fortune* 500 companies have the same types of guidelines, it may be a good time to explore additional ways to promote stock ownership. Based on ECR's analysis, it appears that major U.S. companies are entering the next phase of ownership guideline development—one in which companies have begun taking steps to differentiate their ownership requirements. As such, we've seen companies increase ownership requirements for the CEO and other executives, implement stock retention requirements for those that don't meet ownership requirements, and institute penalties and incentives to achieve guideline compliance.

If the theory is that executives owning company stock helps align their financial interests with those of shareholders, then a larger ownership target or requiring executives to hold stock after vesting may be viewed as helping forge a stronger link. Some companies are already headed in that direction. It will be interesting to see if more companies follow suit.

# Japan's New Corporate Governance Code: Outside Directors Find a Role Under 'Abenomics'

***By David G. Litt***

On March 5, 2015, a Council of Experts formed at the initiative of the cabinet of Prime Minister Shinzo Abe finalized Japan's first Corporate Governance Code (Code). The Code, while nonbinding, should be reflected in revisions to the Tokyo Stock Exchange (TSE) listing rules and related regulations over the next few months that should be in effect as of June 1, 2015, in time for this year's shareholder meetings conducted in Japan during the last two weeks of June.

Although the Code covers a wide ranges of topics and declares a number of sweeping principles, its greatest anticipated immediate impact is that a large majority of Japanese listed companies will nominate and elect two or more outside directors this year, bowing to the Code's requirement to either elect two or more outside directors or explain the reasons for failing to do so at the annual general shareholders' meeting—referred to as the "comply or explain" approach.

## Background

Japanese corporate governance historically operated under a philosophy that gave primacy to employee and customer constituencies, far ahead of shareholders. Nowhere has this approach been more evident than in the composition of boards of directors. As the rest of the world over the past quarter century has emphasized the importance of independent directors—as reflected in numerous corporate governance codes, listing requirements of major stock exchanges and Organisation for Economic Co-operation and Development corporate governance principles—as recently as 2010 only around 40 percent of Japanese companies listed on the First Section of the TSE had even a single outside director.[1]

*Keidanren* (the Japanese Business Federation), Japan's politically powerful lobby of more than 1,000 of the largest Japanese companies, has long opposed mandatory outside director requirements for Japanese companies. *Keidanren* has argued that a board entirely composed of insiders may perform better, and that the unique Japanese institution of a separate board of *kansayaku* (statutory auditors), of which at least a majority must meet an independence test, adequately performs the function of monitoring and supervision on behalf of shareholders.

Despite *Keidanren's* arguments of the merits of insider boards, Japanese companies have performed very poorly on traditional investment measures such as return on equity (ROE), leading to depressed equity valuations evidenced by a low price-to-book ratio (PBR). As reported in one project sponsored by the Ministry of Economy Trade and Industry (METI), in 2012 ROE for Japanese companies averaged 5.3 percent, as against 22.6 percent for US companies and 15 percent for European companies.[2]

Japanese company law was amended in 2003 to allow large companies to opt out of the *kansayaku* system and instead adopt a US-style public company board of directors, with audit, nominating and compensation committees of the board each composed of a majority of outside directors. In Japan this is generally referred to as the "committee system." As of 2013 only 2.2 percent of TSE-listed companies had adopted the committee system, reportedly because of reluctance to cede control to outsiders over the nominating function.[3]

*David G. Litt is a Guest Professor of Keio University in its Faculty of Public Policy Management.*

## Abe-nomics

The government of Prime Minister Shinzo Abe, which came to power in late 2012, has sought to identify and implement structural reforms that can spur investment and economic growth in Japan. These structural reforms are said to constitute the "third arrow" of Prime Minister Abe's economic policy, together with the first and second arrows: fiscal reform and aggressive monetary expansion.

The Abe government quickly identified corporate governance as one area ripe for structural reform, and included the implementation of a system of outside directors in its core June 14, 2013 "Japan Revitalization Strategy." The government's revitalization strategy sees outside directors as necessary to "reform corporate managers' mindset so that they will make proactive business decisions to win in global competition … attaining targets including globally-competitive level in return on equity."[4]

The government's revitalization strategy notes—as have economists—that profitable Japanese corporations have built up excess cash reserves, and insider-dominated boards of directors have typically resisted proactive use of those reserves for new investment, mergers and acquisition, or other strategic realignment. Indeed, economists suggest that improved corporate governance in Japan, as measured by various metrics including board independence, could result in a dramatic reduction in Japanese corporate cash reserves, and the use of these cash reserves can have a significant positive impact on Japan's effort to escape from a long cycle of deflation.[5]

The Abe government has reportedly applied a carrot-and-stick approach in getting the business community to accept its governance proposals, offering a significant cut in corporate income tax rates in exchange for cooperation on new governance requirements, and taking a relatively soft "comply or explain" approach to new requirements, as discussed later.

In November 2013, the government submitted to the Japanese Diet (the national legislature) a bill proposing a change in the Corporation Law to require explanation at a company's annual general meeting of shareholders if the company did not have at least *one* outside director. This "comply or explain" requirement applies to all large companies that are required to have a board of *kansayaku*. The statute also includes a definition of "outside directors" that, although not nearly as broad as, for example, US requirements for audit committee member independence, excludes not only employees of the company, but directors, executive officers, and other employees of a parent company or sister company, and close relatives of directors and executives of the company. The amendment (2014 Amendment) passed into law in June 2014, and went into effect in April 2015.

Significantly, the law that includes the 2014 Amendment also includes a procedural provision calling for review of the corporate governance regime two years after implementation and, based upon the degree of compliance, grants the ability of the government to consider measures that would make inclusion of outside directors mandatory.

The 2014 Amendment also adds to the menu of governance structures a third alternative to (1) the traditional structure of a board composed entirely or mostly of insiders and a separate *kansayaku* board, and (2) the "committee structure." The new, third approach is referred to as a "company with audit committee." Instead of a separate board of *kansayaku*, this audit committee will be formed within and as a committee of the board of directors. It is to be composed of a majority of outside directors and its members separately elected by the shareholders. The audit committee members have full authority as directors, and also have a broader scope of audit authority than the *kansayaku*. It remains to be seen whether a significant number of companies move to this structure, and whether the structure offers a more streamlined or effective alternative to the *kansayaku* board.

Concurrent with legislative deliberations over the 2014 Amendment, the TSE amended its

listed company rules to require companies at least to "make an effort" to include one outside director on the board.

## Role of Institutional Investors

### Foreign Institutional Investors

Foreign ownership of TSE First Section-listed companies is in the 30 percent range by value, though investment is concentrated in larger companies. Foreign institutional investors have enthusiastically supported efforts to add outside directors to boards of Japanese companies.

Institutional Shareholder Services (ISS) at the end of 2011 announced a new Japan policy, effective from 2013, that ISS proxy voting guidelines would recommend a vote against top executive(s) of a company with traditional *kansayaku*-style governance and no controlling shareholder, if the board of directors did not include at least one outside director.

More recently, in June 2014 a large group of foreign institutional investors apparently sent letters to 33 of the largest Japanese companies requesting that they increase to at least one-third outsiders on their boards over three years.[6]

The 2015 ISS proxy voting guidelines likewise caution that, beginning from February 2016, ISS will recommend a vote against top executive(s) of a company with traditional *kansayaku*-style governance and no controlling shareholder, if the board does not include *multiple* outside directors.

### Stewardship Code for Japanese Institutional Investors

If hoarding cash by Japanese corporations presents a near and medium-term macroeconomic issue, poor investment returns on Japanese equities, coupled with continued near-zero interest rates on debt instruments, heighten concerns about the ability of Japan's pension funds to meet commitments to future retirees over a much longer time-frame.

As one way to try and make progress on both fronts, the Abe government tasked a Council of Experts, working with the Financial Services Agency (FSA), to develop a stewardship code of principles for responsible institutional investors, modelled after the UK stewardship code. Japanese institutional investors, historically very passive as shareholders, are requested to disclose whether they accept the Stewardship Code or not. Those who do accept undertake to have clear policies on managing conflicts of interest, monitoring and engaging constructively with investee companies, and to develop "in-depth knowledge of the investee companies and their business environment and skills and resources needed to appropriately engage with the companies and make proper judgments." The investors also must have clear policies on voting, as well disclosing votes and other fiduciary actions to clients and beneficiaries. The Stewardship Code is a call for Japanese institutions to take an active role in corporate governance issues.

The Stewardship Code was finalized on February 26, 2014, and within its first year 184 institutional investors from Japan and abroad had adopted it, including major Japanese trust banks, pension funds, and investment managers.

### Shift in Investment Allocations toward Domestic Equities by the Government Pension Investment Fund (GPIF)

Indeed, the expectation that improved domestic equities performance will help to meet pension obligations was evidenced when, in early November 2014, the behemoth GPIF announced a shift in the allocation of its JPY137 trillion portfolio, more than doubling its target allocation to Japanese equities from 12 percent to 25 percent, while cutting its allocation to Japanese debt from 60 percent to 35 percent. Other government-affiliated pension funds have since made similar shifts.

Meanwhile, prominent Japanese corporations have already been adding outside directors, not waiting for the 2014 Amendment or the corporate governance code to go into

effect. In 2013 Toyota and in early 2014 Canon (whose former president Fujio Mitarai led the opposition to outside director requirements during his 2006–2010 service as chairman of *Keidanren*), each added two outside directors to its board.

## Finally—The Corporate Governance Code

In August 2014, a Council of Experts advised by the FSA and TSE began work on a corporate governance code for listed companies. The exposure draft of the Code was published in December 2014, and the substantially unchanged final version adopted on March 5, 2015.[7]

The Code goes beyond the statutory requirement of the 2014 Amendment by adopting a "comply or explain" standard if a listed company does not have at least two outside directors, instead of one. This responds to concerns that a single outside director cannot be effective in many circumstances. The Code also notes that, if a company decides that it needs to appoint more independent directors, based upon a broad consideration of circumstances, it should disclose a roadmap for doing so.

Although no one was surprised that the FSA served as the secretariat to the Council deliberating on the Stewardship Code for investors, it was seen as significant by many observers that again the FSA—an investor-protection focused regulator—together with the TSE, were designated to serve as the secretariat to the Council of Experts for the Code. Typically changes in the Corporation Law, and related matters of corporate governance, have fallen under the purview of METI-led advisory councils, or even the Ministry of Justice, as was the case with recent policymaking efforts in areas such as guidelines on takeover defenses, regulation of going private transactions, and even the establishment of new types of entities for doing business such as the investment limited partnership. METI is especially close to *Keidanren* and its membership. The location of the Council of Experts at the FSA and TSE drove home the focus upon investor concerns.

How effective will the Code's "comply or explain" be at persuading Japanese corporations to add outside directors? It is too early to say for certain, but an early *Nihon Keizai Shimbun* survey reports that 75 percent of listed companies either plan to appoint at least two outside directors or are studying it. Many fewer, however, expect to have them in place for election at this June's shareholder meetings.[8]

## Conclusion

Of course, all acknowledge that outside directors are not a panacea. Olympus, one of the most significant Japanese corporate scandals in recent history, actually had outside directors on its board as well as two outside *kansayaku* for many years before its financial fraud was revealed (by Michael Woodford, an insider elevated to serve as president of the company). The Olympus outsiders failed miserably. Outside directors will not make much difference if they are not able to access information, if their opinions are not sought, and if they do not have the right training to perform their roles.

Initial anecdotal reports from individuals who have served as outside directors at large Japanese listed corporations suggest there is much room for improvement. The Code has much in it that could prove helpful, outlining the proper role of the board of directors and numerous preconditions for board effectiveness in broad, sweeping language. These provisions should form a solid base for conduct as companies and outside directors find their way.

In the United States, tighter requirements for independent directors in the Sarbanes-Oxley Act and implementing regulations were intended to improve corporate controls, hinder fraud, and generally avoid a repeat of the corruption and scandals that characterized the technology and telecom bubble of 1998–2000. In the Japan of 2015, addition of outside directors to corporate boards is aimed at a very

different goal: to encourage management to be proactive, to encourage risk-taking, and to help boards of directors to make hard decisions that insiders, acting alone, cannot, blocked by webs of personal relationships and groupthink that have developed over many years. The Code at least has the potential to spur these changes, and it is to be welcomed.

## Notes

1. TSE 2013 Listed Companies White Paper on Corporate Governance, pp. 23–29.

2. Ito Review of Competitiveness and Incentives for Sustainable Growth—Building Favorable Relationships between Companies and Investors; Final Report, August 2014, p. 51.

3. *See* TSE-Listed Companies White Paper on Corporate Governance 2013, pp. 15–17.

4. Council of Experts Concerning Corporate Governance Code, Secretariat Explanatory Material, August 4, 2014, p. 1.

5. *See* C. Aoyagi and G. Ganelli, "Unstash the Cash! Corporate Governance Reform in Japan," IMF Working Paper No 14/140, August 2014.

6. *See* "Overseas Investors Demanding More Outside Directors at Japanese Companies," *Nikkei Asian Review*, June 5, 2014.

7. An English language version of the Code is available for download at: *http://www.fsa.go.jp/en/refer/councils/corporategovernance/20150306-1.html*, last accessed March 29, 2015.

8. Morning Edition, *Nihon Keizai Shimbun*, March 6, 2015, p. 2.

# Your Company's Transportation Contracts and FASB's New Revenue Recognition Standard

***By Bob Dow***

The Financial Accounting Standards Board (FASB) recently adopted a comprehensive new accounting standard to overhaul the accepted method of revenue recognition[1] for virtually all industries. The new standard affects the method and timing of recognizing revenue from customer contracts. Companies in the logistics and transportation sector should review their contracts to understand the effect of the new standard on their companies.[2]

## New Revenue Recognition Model

The Standard provides a five-step process for evaluating revenue.

- Identify the contract.
- Identify the separate performance obligations in the contract.
- Determine the transaction price.
- Allocate the price to the performance obligations.
- Recognize revenue.

A contract is not required to be in writing; it may be a practice of dealing with the customer, if it would be legally enforceable. In the context of transportation and logistics, a "contract" may be found in the combination of bills of lading, other shipping documents, INCOTERMs,[3] other standard practices, the course of dealing between the parties, and gap-filler terms provided in the Uniform Commercial Code. Multiple contracts may be combined and treated as one contract if they are sufficiently intertwined. Generally, revenue is recognized as the company satisfies each of its performance obligations.

*Bob Dow is a Partner of Arnall Golden Gregory LLP.*

## Performance Obligations

Understanding the concept of performance obligation is key to managing the revenue recognition process under the Standard. A performance obligation is a promise to transfer goods or services to the customer that can be identified in the contract or implied by customary practices, policies, or specific statements. Customer contracts frequently include multiple performance obligations, which may be bundled into one contract price. The performance obligations must be identified, separated, and accounted for as separate sources of revenue.

Some potential performance obligations in the context of transportation and logistics may include:

- Each mode of transportation of goods (rail, truck, ship, etc.) provided,
- Arranging transportation,
- Supply chain analysis or consulting,
- Tracking of goods,
- Use of software or portals,
- Delivery,
- Storage,
- Insurance,
- Obligations to cover uninsured losses (which could arise from unwritten policies or past practices), and
- Customs clearance.

For a promised good or service to be treated as a separate performance obligation, it must meet both of the following criteria:

- Capable of being distinct because the customer can benefit from the good or service on its own or with other readily available resources, and

- Distinct within the context of the contract, that is, separately identifiable from other promises in the contract.

The following indicators would be used to evaluate whether the good or service is sufficiently distinct:

- Significant integration services are not provided.

- The customer was able to purchase, or not purchase, the good or service without significantly affecting other goods or services in the contract.

- The good or service does not significantly modify or customize another good or service in the contract.

Multiple goods or services may be combined to create a separate performance obligation. If promises cannot be separated according to the previously listed criteria, the contract may be treated as having only one combined performance obligation. If there is only one performance obligation, all revenue recognition is tied to that performance obligation. Depending on the circumstances, this may have the effect of deferring revenue.

Contract modifications must be evaluated to determine whether there is a new performance obligation to be accounted for separately, or whether the entire contract must be reevaluated as to performance obligations and transaction price allocation. This part of the Standard is problematic, and in some cases could result in adjustments of previously recognized income.

Companies providing logistics and transportation services such as those listed above will need to determine whether the services are distinct under the Standard's criteria. In some instances this may turn on whether the services are offered only as a bundled package, and whether the customer could substitute an alternative provider for a particular service.

When the performance obligations are identified, the company must analyze how (1) the contract price is allocated across performance obligations, and (2) each performance obligation is incrementally satisfied so that the revenue for that performance obligation may be recognized in each accounting period.

## Variable Consideration

Another key concept in the Standard is variable consideration. If the price is variable, or there are factors or contingencies that affect the amount of consideration, generally the company must estimate the amounts of expected revenue and only recognize revenue to the extent that it is probable that there will not be a significant reversal of the amounts previously recognized. Prior estimates must be adjusted in each accounting period as the outcome becomes clearer. In its financial statement footnotes, the company must provide a significant amount of disclosure about the variability and any contingencies, as well as a description of the company's methods for estimating the revenue.

## Reporting Revenue on a Gross or Net Basis

The Standard revises the rules governing when a company is treated as acting as a principal (able to report the full, gross amount of revenue) versus acting as an agent (and thus should report revenue on a net basis, deducting payments made to others). Under the Standard, the company must consider certain factors indicating that the company is an agent, including the following:

- Another party is primarily responsible for fulfilling the contract.

- The company does not have inventory risk before or after the goods have been ordered by a customer, during shipping, or on return.

- The company does not have discretion in establishing prices for the other party's goods or services and, therefore, the benefit that the

company can receive from those goods or services is limited.

- The company's consideration is in the form of a commission.
- The company is not exposed to credit risk for the amount receivable from a customer in exchange for the other party's goods or services.

A logistics provider may be acting as an agent when arranging transportation or other services through another provider. In such a case, the Standard may cause the logistics provider to have to start reporting revenues from those services on a net basis.

## Some Additional Concerns Created by the Standard

The implementation of the Standard will raise additional issues for companies in the logistics and transportation sector, including the following:

- *Income taxes.* The company will need to assess the effect on its tax positions; the IRS may require the company to continue to use the old method unless it applies for a change in accounting method.
- *Transfer pricing.* Companies with international operations will need to assess how the Standard affects transfer pricing among business units.
- *Debt covenants.* The change in recognition of revenue may affect the company's compliance with debt covenants.
- *IT systems.* Companies will need to make substantial revisions to their IT systems to capture and record revenue and related information in accordance with the new Standard.

## Clarity is Key

The Standard forces each company to determine, among other things:

- What are its performance obligations?
- How are they satisfied?
- How are they priced (explicitly or implicitly)?
- How will variable consideration be resolved?

The Standard places a premium on clarity in contractual arrangements. Unclear or poorly documented obligations or pricing could yield unpredictable results when applying the Standard to the company's financial statements. Unwritten contractual arrangements could present particularly difficult challenges.

Responding to the new Standard will require a team approach. Management should collaborate with the company's accounting department, sales staff, operations staff, auditors, and legal counsel to assure the best possible outcome.

## Notes

1. Accounting Standards Update (ASU) 2014-09 Revenue from Contracts with Customers (Topic 606) (FASB May 28, 2014) (the Standard), available at *http://www.fasb.org/jsp/FASB/Page/SectionPage&cid=1176156316498*, last accessed March 25, 2015. The Standard is effective for periods beginning after December 15, 2016, for public companies and for annual reporting periods beginning after December 15, 2017, for nonpublic companies, although FASB voted on April 1 to propose a deferral of the effective date of the new revenue standard by one year, but to permit entities to adopt it earlier if they choose. The FASB will issue a formal proposal for a delay, and the public will have 30 days to comment on it before the FASB decides whether to enact it. The Standard with its accompanying commentary, as published, is more than 700 pages long.

2. As noted previously, the Standard is long, and hence dense and complex. This article does not attempt to describe all of its requirements, but merely to highlight some important issues related to each company's contracts.

3. International Commercial Terms, or INCOTERMs, are standardized commercial terms related to the transportation and delivery of goods, published by the International Chamber of Commerce. More information is available at *http://store.iccwbo.org/icc-guide-to-incoterms-2010*.

the Corporate Governance Advisor



## ASPEN PUBLISHERS

76 Ninth Avenue
New York, NY 10011
212-771-0600

Wolters Kluwer

Wolters Kluwer
**The Corporate Governance Advisor**
Distribution Center
7201 McKinney Circle
Frederick, MD 21704

**TIMELY REPORT**

**Please Expedite**

May/June 9900529050