the Corporate Governance advisor

November/December 2012 • Volume 20, Number 6

BOARD OF DIRECTORS

Cognitive Bias in Director Decision-Making

By Delaware Vice Chancellor Travis Laster

I want to speak to you about director decision-making. This topic lies at the heart of the corporate secretary's job: You are the corporate officer most concerned about the care and feeding of the board and most attuned to the art of director decision-making. In particular, I want to focus on cognitive bias. This includes biases such as anchoring and framing. I will use the case method, because that's what we do in law. The case method gives us a set of facts to discuss and lets us examine the mistakes of others, rather than turning the mirror on ourselves.

The case I will use as an example is *In re Southern Peru Copper Corporation Shareholder Derivative Litigation*, a decision that came out in October 2011.[1] If *Southern Peru* doesn't immediately ring a bell, let me provide two facts that will either restore it to your minds or allow you to understand its importance if you somehow missed it. First, the defendants were held liable for $1.347 billion. We don't usually get liability in the Court of Chancery, much less billion dollar judgments. That alone raised eyebrows.

Continued on page 2

Delaware Vice Chancellor Travis Laster delivered this speech during the Society of Corporate Secretaries & Governance Professionals National Conference in July 2012.

Wolters Kluwer
Law & Business

CONTENTS

Second, the plaintiffs were awarded a record $285 million in fees. That is 15% of the post-interest recovery, and represents an effective hourly rate for plaintiffs' counsel of $35,000 an hour for 8,000 hours of work. According to the Wall Street Journal, there have been only three higher fee awards: Enron at $688 million; Tyco at $492 million; and WorldCom at $335 million.

Before anyone in the room goes into cardiac arrest, I should mention that the independent directors were not held liable; summary judgment was entered in their favor. The award was against the controlling stockholder and its representatives on the board.

I will use *Southern Peru* as an example of decision-making on two levels: first, as an example of director decision-making; second, as an example of Chancery Court decision-making.

Some Facts

Southern Peru was a Delaware corporation engaged in mining, smelting, and refining. As its name suggests, its operations were in Peru. Southern Peru was in good financial condition, largely debt free, and performing well. Let's call it the good company. Southern Peru's largest stockholder was Grupo Mexico, a Mexican holding company controlled by Germán Larrea and his family that owned 54.17% of Southern Peru stock. Some of these were high-vote Founders Shares that gave Grupo Mexico a total of 63.08% of the voting power.

Grupo Mexico also owned over 99% of another mining, smelting, and refining company, Minera Mexico. Minera was not in good financial condition, was highly leveraged, and was not performing well. Let's call Minera the bad company. You can probably already see where this is going.

Southern Peru had two other major stockholders: Cerro Trading Company, Inc., which owned 14.2% of the outstanding stock and Phelps Dodge, with 13.95%. Both Cerro and Phelps had held big blocks of Southern Peru stock for some time. They wanted to sell and move on.

If you are a controlling stockholder that owns nearly all of a bad company and a controlling interest in a good company, what might you do? It just might occur to you to sell the bad company to the good company in return for stock in the good company. If you play the valuations right, you end up owning more of the good company.

Sure enough, Grupo Mexico proposed that Southern Peru buy Minera for 72.3 million shares of Southern Peru stock. Grupo Mexico got that number not by some magic formula, but because they took the position that Minera was worth $3.05 billion in cash. That is an important number. It is not only a key fact, but also emblematic of one of the cognitive biases that we will discuss shortly: anchoring.

Southern Peru formed a special committee to evaluate the offer. That was a good thing. The Special Committee was not empowered to negotiate with Grupo Mexico, and could not explore strategic alternatives. Instead, the "duty and sole purpose" of the Special Committee was "to evaluate" the proposal. That was less of a good thing. We will soon see the Special Committee limiting their thinking to their narrow mandate.

The Special Committee was composed of very good people: Harold S. Handelsman, whose resume includes Columbia Law School, Wachtell Lipton, and the Pritzker Group; Luis Miguel Palomino Bonilla, a Wharton Ph.D economist; Gilberto Perezalonso Cifuentes, who holds a law degree and an MBA and has managed multi-billion dollar companies including Grupo Televisa and AeroMexico Airlines; and Carlos Ruiz Sacristán, who served as a Mexican government official for twenty-five years before founding an investment bank. All were A-plus people. The Special Committee also retained A-plus advisors, including Latham & Watkins and Goldman Sachs.

The Special Committee asked Grupo Mexico to put its proposal in writing. Grupo Mexico

responded with the requested term sheet. In the term sheet, the purchase price for Minera remained fixed at 72.3 million shares of Southern Peru stock which, due to changes in the stock price, now were worth $3.147 billion. Critically, at the time the Special Committee evaluated the term sheet, the members believed that Southern Peru could issue 72 million shares in the open market and raise $3 billion in cash. In other words, the Special Committee concluded that there was a real alternative to the Grupo Mexico proposal: Southern Peru could issue stock, get $3 billion in cash, and invest the $3 billion in net-present-value-positive projects.

The Special Committee and its advisors proceeded to evaluate the Grupo Mexico proposal. The materials provided to the Special Committee offer a window into this process. Goldman's first round of materials was very good; they recognized that Grupo Mexico was asking $3 billion for Minera and performed a discounted cash flow analysis to evaluate whether Minera was actually worth the asking price. The initial DCF analysis indicated that Minera was worth only $1.7 billion, or just over half of the ask. Other Goldman analyses, including a comparable companies analysis, indicated that Minera was worth even less than $1.7 billion. In other words, Goldman's standalone value measurements weren't anywhere close to $3 billion. This was a big problem.

Critically, the Special Committee did not use Goldman's initial round of analyses to reject the term sheet, or even to evaluate the alternatives that might be available to Southern Peru if it raised $3 billion in the market. Instead, the Special Committee asked Goldman to go back and see if, with a little more work, they could make the deal happen. The concept tag here is groupthink, or what Chancellor Strine termed "the controlled company mindset."

Subsequently, Goldman made a series of presentations to the Special Committee that abandoned the initial metrics which indicated that Minera's value was nowhere near $3 billion. Never again did the Special Committee see a standalone DCF analysis. Never again did they see a standalone comparable companies analysis. Instead, Goldman decided to value Southern Peru using methods which suggested that Southern Peru's stock was not actually worth its then-current trading price. The apparent logic was that if Southern Peru's stock was overvalued, the company would not be issuing $3 billion in value but actually some lesser amount. Goldman in fact determined that Southern Peru stock was overvalued, a finding which the Special Committee members testified "comforted" them. To reiterate, at this point the Special Committee believed that Southern Peru had a currency—72.3 million shares of stock—that it could use to either raise $3 billion of cash or to buy a company worth $1.7 billion. Rather than using its currency to get $3 billion, the Committee members were "comforted' by the opportunity to rationalize that their currency was not really worth $3 billion. Here, again, we see the Special Committee making cognitive errors: anchoring on their evaluative role, anchoring on the controllers' price, and engaging in groupthink.

Around this time, Goldman began to perform so-called "relative" DCF analyses. Goldman used a range of assumptions for future copper prices, then prepared multiple charts showing the ratio of the value of Southern Peru to Minera under various assumptions. Having examined these books, I can say that they are completely inscrutable. Where you would normally have one chart per page, Goldman put nine charts on a page. The analyses are rife with strange inputs, and nowhere are the underlying assumptions disclosed. Nevertheless, the Special Committee members testified that these analyses "comforted" them. The concept tag here: excessive deference to experts.

Further negotiations then occurred. I won't go through the back and forth. The Special Committee obtained a minor concession in the total number of shares to be issued, which went down to 67.2 million. The Special Committee also secured marginal changes to their deal terms, including a 20 percent collar around the purchase price. Then the Special Committee asked for a majority of the minority voting

condition, a cap on Minera's debt, and various corporate governance provisions. These requests were used as value closers. Candidly, I always worry when I see corporate governance provisions get used as value closers, because nobody knows how to value corporate governance provisions. This tactic is particularly suspect when governance provisions are used to bridge a large valuation gap. I always suspect an effort to save face while caving in.

Grupo Mexico rejected the collar and the majority of the minority condition. The cap on Minera debt was accepted, but it conformed to what Minera was already doing. Finally, Grupo Mexico accepted the corporate governance provisions, but the Chancellor found that the provisions were not materially different from what the post-transaction company would have had anyway. So much for the value of the value closers.

Meanwhile, as part of the final deal, Grupo Mexico offered Cerro and Phelps Dodge liquidity in the form of registration rights in return for their votes. Grupo Mexico made clear that a no vote on the deal meant no liquidity. Both Cerro and Phelps Dodge entered into voting agreements: Cerro agreed to vote in favor if the Special Committee recommended the deal but against if the Special Committee withdrew its recommendation; Phelps Dodge agreed to vote in favor of the deal but was not required to vote against the deal if the Special Committee withdrew its recommendation. During the negotiations culminating in the voting agreements, nobody recognized that Handelsman, as both Cerro's representative on the Southern Peru board and a member of the Special Committee, suffered from a potential conflict of interest. He was supposed to be negotiating the best deal possible and, if necessary, rejecting an unfair deal, but the only way the entity that nominated him could get the liquidity it wanted was if a deal went through.

The final Goldman presentation valued Southern Peru at $3.69 billion based on the company's market capitalization. It valued Minera at $3.146 billion based solely on the market value of the Southern Peru shares that constituted the transaction consideration. The presentation did not include a standalone valuation of Minera. The Special Committee voted 3-0 to approve the merger. Handelsman abstained at the last minute after Goldman belatedly raised his conflict. The merger closed, and Cerro sold its entire interest in Southern Peru with the liquidity rights it had obtained. Litigation ensued, ending with the billion dollar judgment.

An Example of Director Decision-Making

I would first like to examine the *Southern Peru* case as an example of director decision-making. The Special Committee was composed of experienced, competent, and, with the exception of Handelsman, clearly independent directors. The Committee retained top-tier advisors. Yet somehow they blew it. I suggest that *Southern Peru* is an example of cognitive biases at work, where situations distort director thinking. In the language of the opinion, the Special Committee was caught in "the perspective distorting world of deal-making with a controlling stockholder." Someone has to be on the lookout for this.

The cognitive biases I will now discuss are all familiar concepts. The first is anchoring. Anchoring refers to the tendency of people to make estimates based on a known starting value. The starting value can have nothing at all to do with actual value. For example, in one study, people were asked to estimate the number of United Nation member countries in Africa. The study found that if researchers suggested a random number to the subjects, the subjects anchored on that random number to estimate the number of member countries. Anchoring can be useful: it generally makes sense to start with a seller's asking price in a negotiation and push back from that price. But anchoring can also be detrimental: it can distort decision-makers' judgments.

A second cognitive bias is framing. How a problem is framed affects the preferred course

of action. For example, people tend to be risk averse when alternatives are framed as gains, but risk-seeking when alternatives are framed as losses. We don't want to lose what we have, but we are willing to roll the dice to avoid a sure loss.

A third cognitive bias present in *Southern Peru* is confirmation bias. Confirmation bias is the tendency to seek out information that validates existing views and prior commitments. Confirming evidence makes us feel good, so we embrace it. At the same time, we seek to discount and explain away disconfirming evidence. We tell a story in our minds, then attempt to fit the evidence to our story. As a judge, I have to be particularly vigilant against confirmation bias.

The final cognitive bias I will discuss is groupthink. Groupthink is the most important bias for boards of directors to watch for. People inherently desire harmony and tend to avoid speaking out. No one likes to make waves in a group. Dissent does not have to be suppressed with an iron fist; it can be suppressed more easily through social ties. People even self-suppress: they avoid raising matters that are uncomfortable and don't speak up for fear of looking like a moron in front of their peers.

The term groupthink was coined by Irving Janis as part of his analysis of John F. Kennedy's decision-making. Janis noted significant differences in how Kennedy approached the Bay of Pigs fiasco and the Cuban Missile Crisis. In 1961, the CIA presented a plan to Kennedy for a landing at the Bay of Pigs that they had been developing since the 1950s. The CIA was emotionally invested in that plan. Alan Dulles, a high-prestige figure at the time, argued in favor of the landing. Other alternatives were not presented; it was a go/no-go decision. The CIA representatives dominated the discussion, and Kennedy's other advisors showed deference to the CIA representatives as experts. The few objections that were raised were explained away. Kennedy, the ultimate decision-maker, was present for the entire discussion. His presence added an unspoken pressure to avoid dissent: nobody wanted to speak up and risk looking like a moron in front of Kennedy.

A year later, during the Cuban Missile Crisis, Kennedy used a much different approach. Having learned from the Bay of Pigs fiasco, Kennedy intentionally absented himself from the initial meetings to encourage free discussion. Everyone was expected to contribute, not just the experts. There was an effort to develop multiple options. Two teams were created to evaluate the principal options, an airstrike and a blockade. Each team pitched their plan to Kennedy in front of the other team, and the teams debated the merits of their plans in front of Kennedy. Only after hearing a vibrant debate did Kennedy make a decision. Let's keep the Kennedy examples in mind as we explore the cognitive biases in *Southern Peru*.

The first cognitive bias present in *Southern Peru* is anchoring. The Special Committee received a narrow mandate to vote up or down on the transaction. It was clear that the controller wanted the transaction, and that the $3 billion offer was a hard number. The Special Committee anchored off that number, focused on the proposed transaction, and gave no thought to what else could be done with the $3 billion.

The next cognitive bias is confirmation bias. The initial analyses of Minera's standalone value were radically inconsistent with both the $3 billion anchor and with the idea that the merger was a good deal for Southern Peru. The Special Committee responded by discarding the uncomfortable valuation evidence and asking Goldman to develop more comfortable, but unconventional, analyses which generated results that conformed to the Special Committee's desire to get the deal done. The Special Committee then accepted the later analyses despite their weaknesses. Confirmation bias was at work.

The acceptance of Goldman's inscrutable analyses demonstrates yet another cognitive bias: excessive reliance on experts. I would be shocked if any director understood them. I would also be shocked if any Special Committee member raised their lack of understanding with their fellow members. I suspect what happened was that the analyses looked pretty, were

presented in a nice book, and generally looked smart and official. They were accepted without any hard questioning.

The final cognitive bias evidenced in *Southern Peru* is framing. What happens over the course of a deal is that participants catch "deal fever." They have been working on a transaction for a long time and want to see it accomplished. Failing to close the deal feels like a loss, and participants engage in risk-seeking behavior in order to get the deal done and avoid suffering the pain of that loss. Deal participants make the biggest concessions as the time for signing looms because they want to avoid losing the deal.

As a judge, I am constantly aware of the need to fight cognitive bias. I am constantly trying to figure out what expectations I have going into a situation and whether those expectations are valid. What saves me most of the time is that I have two sets of excellent lawyers trying to beat each other's brains out. Just as Kennedy had two teams arguing alternative proposals to address the Cuban Missile Crisis, I have two sets of lawyers attempting to convince me that their side's proposal is good and the other side's proposal is bad. That is the best protection I have.

Recommendations

As the people most responsible for the care and feeding of the board, corporate secretaries should recognize the ever-present need to fight cognitive bias. I would encourage you to create protective processes for the board.

All of your directors will be aware of cognitive bias. Nothing I have said here is anything new. But you can't review it often enough.

First, I suggest that once a year you invite a scholar to make a presentation on cognitive bias. Most of your companies are near a college or university that houses a scholar who does research on decision-making. I would encourage you to ask that scholar to present a case study of a company like yours that blew it. Have her come in and talk about a decision that seemed great at the time, but now, with the benefit of hindsight, was clearly based on premises that were insufficiently tested. Have her talk about New Coke.

Second, always recognize the need to decide how to decide. While this may sound trite, the difference between Kennedy's approach to the Bay of Pigs and the Cuban Missile Crisis was a product of careful thinking about how to decide. After the Bay of Pigs, Kennedy examined how the decision to invade was made. He asked himself: "What can I do to avoid repeating errors in the decision-making process?" This type of reflection is crucial in the boardroom as well. Granted, recent years have seen improvements in board decision-making. Executive sessions are a fine example: they are crucial protectors against cognitive bias. Executive sessions take one of the major policers of dissent out of the equation. I'm not saying that CEOs are actively suppressing dissent, but their presence injects subconscious pressure to avoid speaking up on controversial issues. The executive session largely eliminates that problem.

Third, collegiality in the boardroom is great, but don't overvalue it. Too much collegiality blends into groupthink. Constructive conflict produces better decision-making. It is obviously not great to have bomb-throwers in the boardroom that disagree with everything. But it is also not great to have everybody agreeing with everything, nodding their heads, and not asking questions. I've heard it said that every board needs an SOB. You want the SOB to know when not to be an SOB, but you also want the SOB to ask the CEO the tough question about a proposal, to ensure that the proposal on the table has been properly vetted, and to insist on alternatives.

If you don't have an SOB in your boardroom, appoint a designated devil's advocate. Have the appointment rotate. I was on a non-profit board that, instead of a devil's advocate, appointed a designated "process observer." The process observer's role was to observe the discussion and note when the board either was becoming

inactive and acting excessively deferential to the executive director or, on the other hand, attempting to micromanage the affairs of the organization. A designated devil's advocate or process observer is a great way to take the pressure off the remainder of the board and to create an institutionalized deterrent to groupthink.

Fourth, the board must be involved in discussing alternatives to a given course of action. Advisors love to have an advisors' call with management before the board call. That way, by the time of the board call, advisors and management can present a united front to the board. All of the fun stuff—the outside-the-box thinking, testing, and debate about alternatives—happens on the advisors' call. Presenting a united front to the board is a great way for advisors and management to save face, but it is definitely not good for board decision-making. The board needs to hear the debate and discuss the alternatives. The board needs structures that will encourage debate and discussion.

Last, seek out informed generalists. I'm not suggesting that corporations abandon the grids on board expertise that help ensure diversity in the boardroom. But the informed generalist brings something perhaps even more important than depth of expertise in a particular field: common sense. One of the lessons that Kennedy drew from the Bay of Pigs was the danger of overreliance on experts. Overreliance on experts is a phenomenon that we see in the M&A context all the time. The informed generalist has the ability to draw on experience from other settings and say "I may not know a lot about this particular topic, but this just doesn't make a lot of sense." In the context of *Southern Peru*, the informed generalist might have asked "Why would we use $3 billion to go out and buy something worth $1.7 billion?" Find yourselves some informed generalists.

Southern Peru as an Example of Chancery Decision-Making

Let me shift gears and explain how *Southern Peru* is also an example of Chancery decision-making. The takeaway here is simple: we actually look for cognitive bias. *Southern Peru* is a case that involved entire fairness, our strictest standard of review. People love to make Delaware law complex—"You're not in *Revlon*, you're in *Blasius*. No, you're in *Unocal*. No, no, you're in entire fairness!"—but we actually only have three standards of review. The three standards form a declining pyramid of deference.

At the bottom tier of the pyramid is the business judgment rule. Under the business judgment rule, we won't second-guess your decision unless it is so wacky that it is unjustifiable on any grounds. Put differently, something has to stink so badly that we feel compelled to dig deeper and determine what motivations lie underneath. We call this waste. Waste is not a separate standard—it simply means "beyond the business judgment rule." Waste is met when you look at something and it seems so messed up that you cannot accept the decision at face value. Waste is the legal embodiment of the proverbial smell test. In business judgment land, our sense of smell is not very good. We give wide deference to the decisions of independent, disinterested directors, particularly when they own stock so that their incentives are aligned with those of the stockholders.

The next level of the pyramid is enhanced scrutiny. When you are in the type of recurring situation where we know that cognitive bias tends to arise, we ask whether your decision is reasonable. For example, if a hostile bidder rolls in and wants to buy a company, but the CEO does not want to go, the directors tend not to want to go either. They take defensive measures—adopting a poison pill or pumping a block of stock to a friendly investor. These measures could just as easily be taken to serve their self interest rather than the interests of the corporation. The same actions also could be consistent with their fiduciary duties. The potential for cognitive bias is rife. The directors are likely close with the CEO. They could be anchoring off personal views of the value of the company. They could be framing the takeover as a loss of independence and therefore be more willing to take a risk on the CEO's plan. To address these

concerns, we apply enhanced scrutiny and ask whether a decision is reasonable.

At the top of the triangle is entire fairness. Entire fairness scrutiny is only employed in situations where there is a direct conflict. When we apply entire fairness, we ask whether you got it right. More formally, we ask whether the challenged conduct was entirely fair to the corporation as to process and as to price. In the entire fairness setting, you often see situations akin to *Southern Peru*: good people who tried hard but did things that don't make much sense. The Chancellor applied entire fairness scrutiny to the Special Committee's decisions in *Southern Peru*. Each time a decision came up, the Chancellor asked "why did they do this?" If the explanation appeared to be tainted by cognitive bias, or to be even more nefarious, he dug deeper. *Southern Peru* came out the way it did because of the standard of review and a series of seemingly biased decisions.

The last thing I want to discuss is the record that the Special Committee made for the Court. I view the corporate secretary as the keeper of the board materials and the minutes. We already discussed Goldman's board materials. We haven't discussed the minutes. That's because they were not produced during discovery and were therefore excluded. It is not clear from the opinion what happened—whether they were not prepared in time or just not found. I had a case where the critical minutes were prepared a year after the meeting by someone who had not even attended. That was not confidence inspiring.

Board materials and minutes are extremely important in litigation. When you are a practicing attorney advising a board, you attend every meeting and know whether the directors have done a good job. You know that the director who was the childhood friend of the CEO and has been on the board for fifteen years actually asked the toughest questions. You can legitimately represent to the court that the directors did a great job and acted in utmost conformity with their fiduciary duties. But the judge has not had any of that access. And the lawyers tell the court that there is no problem in every case. All the judge has to rely on are things like minutes, board materials, contemporaneous notes, and emails to gain insight into what actually occurred. The board materials and minutes should help confirm in the judge's mind that a good process was followed and that there were no cognitive biases at play.

The best M&A board books I've seen discuss alternatives. They do not just present the board deliberations as a go/no-go on the sale decision. The minutes should also reflect discussion. Minutes should not be verbatim, but they should do more than provide a list of topics. More importantly, a bare list is not helpful to a director in deposition. Many times in deposition, a director will answer "I don't recall, but I'm sure it's in the minutes." Then, when the attorneys go to the minutes, they read only "discussion ensued." The only person these minutes help is the person writing them—they were able to save time by writing less. Writing good minutes is like flossing: nobody likes to do it, but it is essential for good hygiene.

Conclusion

Southern Peru is an example of our effort to find out what went on in the boardroom. We do not think that most people are bad or avaricious. In fact, under the business judgment rule, there is a presumption that the people running companies are good people trying to do the right thing. But we recognize that good people are often blinded, wholly or in part, by cognitive biases. When that happens, you generally get decisions that result in equitable remedies such as injunctions rather than personal liability. But in controller situations like *Southern Peru*, cognitive biases can result in liability—here, a $1.4 billion judgment.

As a judge, I have to check myself for cognitive biases every time I write an opinion. I recommend you remember cognitive biases when you think about director decision-making.

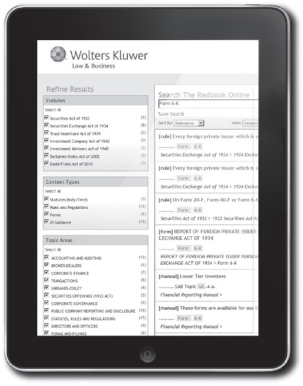
Do the directors know about these biases? Of course they do. But they need to be reminded. It is your role as corporate secretaries to help police the decision up front, to assist the board in making the decision, and to reflect the decision in the minutes. In that role, you should remind the board of cognitive biases. That way, by the time you come to me, the documentation will reflect a considered director decision-making process that I will be happy to respect.

Note

1. On August 27, 2012, the Delaware Supreme Court upheld Chancellor Leo Strine's October 2011 trial decision in the Southern Peru Copper case. *Americas Mining Corporation, et al. v. Michael Theriault,* No. 29, 2012 (Del. Aug. 27, 2012).

Introducing RBsource, the all-in-one online securities law resource, powered by The Securities Red Book.

The new RBsource completely re-imagines the industry-standard *Securities Red Book* to give you a more intuitive, smarter, web-based tool that better meets your needs. With RBsource, you get:



- **An authoritative resource:** RBsource takes the trusted content of *The Securities Act Handbook* and integrates SEC guidance and interpretations — available anytime, anywhere, on any device
- **An intuitive resource:** Customize your work environment and search by keyword or browse and filter results by statute, content type (laws, regs, forms and guidance), or by practice matter topics
- **An intelligent resource:** RBsource "thinks" right along with you, uniquely associating all related content — from forms, statutes, and regulations to related SEC guidance and interpretations
- **A timely resource:** RBsource is updated daily, providing you with changes to rules and regulations every time you log in

Sign up for a 14-day FREE trial now!

Visit RBsourceWK.com

Wolters Kluwer
Law & Business

Cybersecurity Disclosure: SEC's Expanding Disclosure Initiatives & Expectations

By Andrew Gerber and Janet Lowder

In response to a May 2011 letter[1] from Senator John Rockefeller and four other senators to Securities and Exchange Commission (SEC) Chairwoman Mary Schapiro, the SEC issued CF Disclosure Guidance: Topic No. 2 - Cybersecurity (the "SEC Guidance") on October 13, 2011.[2] The authors of the Rockefeller letter emphasized that the cybersecurity risks of many companies were not well understood, referencing their view that a "substantial" number of public companies provided no information regarding cyber issues and those that did provide some information, often used generic language.[3] The apparent goal of the Rockefeller letter was to require that companies routinely and fully disclose "information on [the] steps taken by companies to reduce [cybersecurity] risk exposure."[4]

While the SEC has not formally adopted a rule related to cybersecurity, its guidance issued in response to the Rockefeller letter, coupled with the comment letter process of its Staff, effectively creates a disclosure standard. Consequently, cybersecurity issues should be considered by all companies in preparing disclosures as failure to properly report on this topic could lead a company to run afoul of current SEC reporting rules, including the antifraud provisions found in Exchange Act Section 10(b) and Exchange Act Rule 10b-5. This article addresses: (I) the SEC's Guidance in CF Disclosure Guidance Topic No. 2 - Cybersecurity; (II) SEC Comment Letter Trends; (III) Sample Disclosures; and (IV) Current Legislative Initiatives.

Andrew A. Gerber is a Partner of Womble Carlyle Sandridge & Rice LLP and Janet D. Lowder is an associate of Womble Carlyle Sandridge & Rice LLP. The opinions expressed in this article are the authors' own and do not necessarily reflect the opinions of their firm or any of its clients.

SEC Guidance in CF Disclosure Guidance Topic No. 2 - Cybersecurity

What does cybersecurity cover?

Cybersecurity is "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access."[5] In the SEC's view, cyber incidents include those resulting from both intentional and unintentional actions and involve unrelated third parties and company insiders. Examples of cyber attacks include

- "gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data";

the Corporate Governance Advisor

The ***CORPORATE GOVERNANCE ADVISOR*** (ISSN 1067-6171) is published bimonthly by Aspen Publishers at 76 Ninth Avenue, New York, NY 10011. Subscription rate, $625 for one year. POSTMASTER: Send address changes to *THE CORPORATE GOVERNANCE ADVISOR,* Aspen Publishers, 7201 McKinney Circle, Frederick, MD 21704. Send editorial correspondence to Aspen Publishers, 76 Ninth Avenue, New York, NY 10011. To subscribe, call 1-800-638-8437. For Customer service, call 1-800-234-1660.

- "causing operational disruption"; and
- "causing denial-of-service."[6]

In producing disclosure, a company should consider and evaluate all costs associated with any cyber breach, including those associated with

- remediation;
  - costs associated with stolen assets and
  - costs to retain business following compromised information
- increased cyber protection;
- organizational and personnel changes to protect against future attacks;
  - increased employee training costs and
  - costs to retain third party consultants or purchase cybersecurity products
- lost revenues;
- litigation; and
- reputational damage.

No Explicit Disclosure Rules

The SEC acknowledges that no existing SEC rule or regulation specifically requires disclosure of a company's cybersecurity risks or cyber incidents. The SEC's guidance on this topic stems from the general disclosure requirements found in existing regulations such as Securities Act Rule 408, Exchange Act Rule 12b-20, Exchange Act Rule 14a-9 and Regulation S-K Items 101, 103, 303, 307 and 503(c). As with all other disclosures, information that would be required by a reasonable investor to make an investment decision or that would alter the total mix of information available must be reported.[7]

In addition, the antifraud provisions found in Exchange Act Section 10(b) and Exchange Act Rule 10(b)-5, which require the disclosure of any material information necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading, also applies to the area of cybersecurity. While the SEC emphasizes the need for disclosure of cybersecurity issues in the SEC Guidance, it also states twice that a company's cyber related disclosures may be limited and do not need to be so specific as to compromise the company's security. Given the lack of specific disclosure rules, each company must continuously apply a facts and circumstances test to its given situation to determine whether disclosure, if any, is required.

Areas of Disclosure in SEC Filings

The SEC highlights five disclosure areas where a discussion of cybersecurity matters may be appropriate. While this list is not exhaustive, it provides a helpful start to companies in determining the appropriate venue for disclosure.

Risk Factors. Item 503(c) of Regulation S-K requires the disclosure of factors that make investment in a company speculative or risky. Risk factor sections commonly appear in Form 10-Ks, certain proxy statements and registration statements, such as those on Form S-1 and Form S-3. Only disclosure of significant risks is required, and disclosure should not be overly broad or generic but specifically tie the risk to the company and its business. Further, the SEC makes clear that, if a material[8] cyber incident has occurred, a company should refer to the incident and related costs and consequences in its risk factors rather than referring to the potential for such an event.

In deciding whether a cybersecurity related risk factor is appropriate, companies should evaluate:

- their cybersecurity risks, giving consideration to "all available relevant information, including prior cyber incidents and the severity and frequency of those incidents";

- "the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks"; and

- "the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which [the company] operate[s] . . . including threatened attacks . . . ."[9]

Sample risk factors may relate to: (1) "aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences"; (2) the outsourcing of cyber related functions; (3) actual cyber incidents, whether individually material or material when considered in the aggregate; (4) undetected cyber incidents; and (5) insurance coverage.[10]

MD&A. A company should discuss cybersecurity risks and incidents in its MD&A if the costs or consequences associated with known or potential incidents "represent a material event, trend or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition."[11]

Description of Business. A company should discuss cyber related incidents in its description of business when such incidents materially affect its "products, services, relationships with customers or suppliers, or competitive conditions," giving consideration as to how such incidents affect the company's reportable segments.[12]

Legal Proceedings. Material litigation or other legal proceedings that relate to a cybersecurity matter must be disclosed.

Financial Statement Disclosure. The costs and impairments associated with cyber incidents must be appropriately accounted for in a company's financial statements and documented in the corresponding notes.[13]

Disclosure Controls and Procedures. When making Regulation S-K Item 308 certifications regarding the company's disclosure controls and procedures, the CEO and CFO should consider cyber incidents to the extent they pose a risk to the company's "ability to record, process, summarize, and report information that is required to be disclosed in [SEC] filings . . . ."[14]

Enhanced Disclosure Through the SEC Comment Letter Process

Since October 2011, the SEC has issued numerous comment letters pertaining to cybersecurity issues. Comments have been given to companies across all industries.[15] SEC comments have predominantly arisen in the context of Form 10-K reviews, but the SEC has also reviewed this disclosure in other filings such as Form S-1[16] and Form 20-F.[17] As discussed further below under "Comment Letter Response Trends," even when a company determines a cybersecurity related matter is immaterial and does not rise to the level of disclosure in its SEC filings, the SEC, through its comment process, on multiple occasions has effectively overruled the company's determination and required disclosure.

Attacks and Breaches

While the SEC has requested some companies to generally consider how cybersecurity issues affect their businesses and SEC disclosures on the whole,[18] most comments have focused on risks factors - specifically the expansion of risk factors. Notably, the SEC has repeatedly requested companies to acknowledge actual cyber attacks, breaches and similar incidents within their risk factors regardless of whether such attack, breach or incident, alone or aggregated with other such instances, is deemed material. However, the SEC has generally not required companies to reference the details of specific attacks, breaches or similar events.

For instance, in a Staff Comment Letter dated April 5, 2012 to The Hartford Financial Services Group,[19] the SEC asked whether Hartford had "experienced a virus or other malicious code, unauthorized access, a cyber attack or other

computer related violation in the past," given the stated dependence of its business on its ability to access certain computer systems, "and, if so, whether disclosure of the fact would provide the proper context for [its] risk factor disclosures."[20] Hartford initially responded[21] that it had not experienced a material cybersecurity breach, to which the SEC replied,[22] "despite the fact you believe you have not experienced a material breach of your cybersecurity, are you currently experiencing attacks or threats to your systems? If you have experienced attacks in the past, please expand your risk factor in the future to state that."[23] Thus, regardless of whether a cyber attack was material, Hartford was called to address previous attacks in the context of its risk factor disclosure. Hartford agreed to update its disclosure going forward, saying it has been and will likely be subject to cyber attacks, although none to date have been material.[24] See "Sample SEC Disclosures" below for Hartford's sample risk factor.

Likewise, in a letter to Aon Corporation dated April 12, 2012,[25] the Staff asked whether Aon had "experienced a computer virus, security breach, cyber attack or other computer related violation in the past."[26] Aon responded[27] that the cybersecurity breaches it experienced all occurred in the ordinary course of business, were not unique to its business and none, individually or in the aggregate, were material to the company's operations. Despite the lack of materiality, the SEC called Aon to include reference to the breaches in its disclosures going forward.[28]

Similarly, in Spring 2012 correspondence with The Western Union Company, Western Union agreed to add a cybersecurity risk factor, although"[n]one of the attacks or breaches [questioned by the SEC] has individually or in the aggregate resulted in any material liability"[29] to Western Union, and also agreed to state that it had been the subject of cyber attacks in such risk factor.[30]

Third Party Vendors

The SEC has also required companies to disclose cybersecurity breaches and other incidents occurring at third party vendors. For example, through correspondence with CIT Group,[31] a "few data security incidents of third party vendors that impact CIT Group customers" were identified.[32] The SEC called CIT Group to "clearly state in [its] risk factor that [its] third party vendors have experienced attacks that affected some of [its] customers."[33] The SEC noted, however, that CIT Group "may include language that indicates that the attacks were mitigated."[34]

Where is the SEC looking for information?

In a somewhat unprecedented review expansion, the SEC has, on several occasions, looked outside of the specific filing on which it is commenting and considered not only other company filings but also company related statements, peer disclosures and industry articles. Using such outside information, the SEC has looked to tie its findings back to individual issuers.

Past SEC Filings. In a **May 2012** comment letter, the SEC looked back to Google's **January 2010** filing of a Form 8-K that disclosed a cyber attack as the basis for requiring Google to update its cybersecurity risk factor "to state that in the past you have experienced attacks."[35]

Company Websites. In commenting on Amazon.com's 2011 annual report on Form 10-K,[36] the SEC surveyed a subsidiary's website, Zappos.com. The Zappos.com website announced that a cyber attack occurred that compromised millions of user accounts, although Amazon's risk factors did not reference this occurrence. The SEC Staff saw the Zappos.com statement and referenced it in their comments to Amazon. The SEC indicated that it was not enough to warn investors of cyber attacks but that Amazon must disclose the occurrence of cyber attacks in its risk factors.

Employee Comments. In going a step further, comments made by employees of Intel Corporation[37] and Eastman Chemical Company[38] also led to comments from the SEC and, in the case of Eastman, a demand for increased cybersecurity disclosure. In Intel,

the Vice President and General Manager, Data Center and Connected Systems Group was quoted as saying that the IT and data security "environment we are all living in just continues to increase in intensity. The number of attacks to our environment is doubling every year. The sophistication of those attacks is getting more intense."[39] In Eastman, a non-management employee had made "several recent public statements . . . regarding the importance of cybersecurity and the implementation of control systems in the chemical sector to protect the sector from cybersecurity threats."[40]

Peer SEC Filings. The SEC examined peer disclosures in asking Texas Instruments Incorporated[41] to explain why it had not included specific cybersecurity disclosures in its annual report on Form 10-K when peer companies included such disclosure. Texas Instruments agreed to add cybersecurity disclosure in response to the comment.

Industry News. In perhaps the farthest reaching example, the SEC looked to a "recent news article" concerning credit card phishing scams in commenting on Shinhan Financial Group Co. Ltd's Form 20-F.[42] The SEC asked Shinhan to tell them what consideration was being giving to expanding risk factor coverage. In response, Shinhan agreed to add a risk factor regarding phishing in future filings.

Comment Letter Response Trends

It should be noted that upon receiving a request for expanded disclosure, many companies have replied to the SEC that they have considered the issue and not found it to rise to a material level requiring disclosure and/or that their current disclosures comply with SEC rules and regulations. To such responses, the SEC frequently reaffirms its comment, posing it on second or third instance not as a question or request for information but a requirement for a specific disclosure. Most companies receiving a cybersecurity related comment appear to have ultimately agreed to some level of revised disclosure. The Hartford Financial Services Group, Amazon.com, Aon Corporation and CIT Group are all companies that initially sought to characterize cybersecurity disclosures as immaterial to their businesses in response to SEC request for additional disclosure only to be required to make expanded disclosures going forward.[43]

Timing of Revised Disclosure

Another interesting point arising out of the comment letters relates to timing of revised disclosure. Most comment letters appear to require the new disclosure going forward and not as an amendment to the current filing. The SEC may either reference the inclusion to be "in future filings" or in the company's next quarterly report on Form 10-Q. When the SEC has stated that the disclosure should be amended in the company's next quarterly report on Form 10-Q, most companies appear to have complied. However, at least one, Honeywell International, indicated that it did not plan to provide the revised risk factor in its next Form 10-Q citing "Item 1A of Part II – Other Information of Form 1-Q [that] requires the inclusion of 'any *material* changes from risk factors as previously disclosed . . .' (emphasis added)" when Honeywell did not view the requested change "a 'material change' to [its] existing cybersecurity risk factor."[44] The SEC declined to comment further on this approach. Thus, there appears to be some precedent for a company's request to temporarily defer an update to disclosure until its next annual report versus quarterly report – even if the SEC initially requests the update in the quarterly report – where a company continues to maintain that such disclosure is non-material.

Sample Disclosures

The majority of companies have addressed cybersecurity issues raised by the SEC Guidance in risk factors required by Item 503(c) of Regulation S-K. To date, fewer companies appear to have included discussion of cybersecurity matters (excluding companies providing cyber protection services) in their MD&A, business description, legal proceeding disclosure or as notes to their financials. The variety and

depth of disclosure remains widely disparate, although due to the numerous SEC comment letters this year and the subsequent agreement by many companies to increase disclosures going forward, it appears that the trend and SEC mandate will be for more fulsome and specific disclosure in future filings, especially during the next season of annual reporting.

A few examples of how companies have revised risk factor risk disclosure in light of SEC comments follow.

The Hartford Financial Services Group

In response to SEC probing, The Hartford Financial Services Group[45] indicated that it had been the subject of cyber attacks and threats. Because of this admission, per the SEC's instructions, it will be required to include language in its cybersecurity related risk factor going forward to state that it has been subject to attacks. Hartford included the revised risk factor in its quarterly report on Form 10-Q for the quarter ended June 30, 2012. As revised, the risk factor added three sentences that acknowledge that Hartford's computer systems "have been, and will likely continue to be, subject to computer viruses or other malicious codes," mitigate the occurrence of such incidents by stating that it had "not experienced a material breach of cybersecurity" and address the fact that it purchases insurance to cover such incidents. The revised risk factor is shown below.

If we are unable to maintain the availability of our systems and safeguard the security of our data due to the occurrence of disasters or a cyber or other information security incident, our ability to conduct business may be compromised, we may incur substantial costs and suffer other negative consequences, all of which may have a material adverse effect on our business, financial condition, results of operations and liquidity.

We use computer systems to process, store, retrieve, evaluate and utilize customer and company data and information. Our computer, information technology and telecommunications systems, in turn, interface with and rely upon third-party systems. Our business is highly dependent on our ability, and the ability of certain third parties, to access these systems to perform necessary business functions, including, without limitation, conducting our financial reporting and analysis, providing insurance quotes, processing premium payments, making changes to existing policies, filing and paying claims, administering variable annuity products and mutual funds, providing customer support and managing our investment portfolios and hedging programs.

Systems failures or outages could compromise our ability to perform our business functions in a timely manner, which could harm our ability to conduct business and hurt our relationships with our business partners and customers. In the event of a disaster such as a natural catastrophe, a pandemic, an industrial accident, a blackout, a terrorist attack or war, systems upon which we rely may be inaccessible to our employees, customers or business partners for an extended period of time. Even if our employees and business partners are able to report to work, they may be unable to perform their duties for an extended period of time if our data or systems used to conduct our business are disabled or destroyed.

Moreover, our computer systems have been, and will likely continue to be, subject to computer viruses or other malicious codes, unauthorized access, cyber-attacks or other computer related penetrations. While, to date, The Hartford has not experienced a material breach of cybersecurity, administrative and technical controls as well as other preventive actions we take to reduce the risk of cyber incidents and protect our information technology may be insufficient to prevent physical and electronic break-ins, cyber-attacks or other security breaches to our computer systems. Such an event could compromise our confidential information as well as that of our clients and third parties with whom we interact, impede or interrupt our business operations and may result in other negative consequences, including remediation costs, loss

of revenue, additional regulatory scrutiny and litigation and reputational damage.

In addition, we routinely transmit, receive and store personal, confidential and proprietary information by email and other electronic means. Although we attempt to keep such information confidential, we may be unable to utilize such capabilities in all events, especially with clients, vendors, service providers, counterparties and other third parties who may not have or use appropriate controls to protect confidential information.

Furthermore, certain of our businesses are subject to compliance with regulations enacted by U.S. federal and state governments, the European Union, Japan or other jurisdictions or enacted by various regulatory organizations or exchanges relating to the privacy of the information of clients, employees or others. A misuse or mishandling of confidential or proprietary information being sent to or received from an employee or third party could result in legal liability, regulatory action and reputational harm.

Third parties to whom we outsource certain of our functions are also subject to the risks outlined above, any one of which may result in our incurring substantial costs and other negative consequences, including a material adverse effect on our business, financial condition, results of operations and liquidity.

While we maintain cyber liability insurance that provides both third party liability and first party insurance coverages, our insurance may not be sufficient to protect against all loss.

Amazon.com

As an Amazon.com[46] subsidiary, Zappos.com experienced a documented cybersecurity breach that compromised customer information. The SEC required Amazon to amend its cybersecurity risk factor going forward to disclose that it had experienced cyber attacks and breaches and to state that it relies on third party technology and support. In response, Amazon amended its risk factor to include expanded disclosures regarding its use of third party vendors and the related risks and specifically state "[s]ome subsidiaries had past security breaches."[47] This disclosure was included in its quarterly report on Form 10-Q for the quarter ended June 30, 2012. The changes made in response to the SEC's comments are shown below.

As a result of our services being web-based and the fact that we process, store and transmit large amounts of data, including personal information, for our customers, failure to prevent or mitigate data loss or other security breaches, including breaches of our vendors' technology and systems, could expose us or our customers to a risk of loss or misuse of such information, adversely affect our operating results, result in litigation or potential liability for us and otherwise harm our business. We use third party technology and systems for a variety of reasons, including, without limitation, encryption and authentication technology, employee email, content delivery to customers, back-office support and other functions. Some subsidiaries had past security breaches, and, although they did not have a material adverse effect on our operating results, there can be no assurance of a similar result in the future. Although we have developed systems and processes that are designed to protect customer information and prevent data loss and other security breaches, including systems and processes designed to reduce the impact of a security breach at a third party vendor, such measures cannot provide absolute security.

Kellogg Company

In response to the SEC's request for Kellogg Company[48] to state whether it had been the subject of cybersecurity breaches in the past, Kellogg added language to its cybersecurity risk factor to state that its computer systems "have been, and will likely continue to be subjected to computer viruses."[49] Kellogg went on to describe the negative impact these attacks could have but also mitigated the impact of such attacks by stating that "[t]o date, we have not experienced a material breach of cybersecurity"

and indicating that they have special controls and take preventative actions to ward against these threats.[50] Kellogg's revised risk factor is below.

Technology failures could disrupt our operations and negatively impact our business.

We increasingly rely on information technology systems to process, transmit, and store electronic information. For example, our production and distribution facilities and inventory management utilize information technology to increase efficiencies and limit costs. Furthermore, a significant portion of the communications between our personnel, customers, and suppliers depends on information technology. Our information technology systems may be vulnerable to a variety of interruptions, as a result of updating our SAP platform or due to events beyond our control, including, but not limited to, natural disasters, terrorist attacks, telecommunications failures, computer viruses, hackers, and other security issues. Moreover, our computer systems have been, and will likely continue to be subjected to computer viruses or other malicious codes, unauthorized access attempts, and cyber- or phishing-attacks. These events could compromise our confidential information, impede or interrupt our business operations, and may result in other negative consequences, including remediation costs, loss of revenue, litigation and reputational damage. To date, we have not experienced a material breach of cybersecurity. While the Company has implemented administrative and technical controls and has taken other preventive actions to reduce the risk of cyber incidents and protect our information technology, they may be insufficient to prevent physical and electronic breakins, cyber-attacks or other security breaches to our computer systems.

Current Legislative Initiatives

The Administration introduced a legislative package to Congress in May 2011[51] that led to the SEC's increased focus on cybersecurity disclosures. Since that time, Administration officials have testified 17 times on the subject and presented over 100 briefings.[52] In April of this year, the House passed a Cyber Intelligence Sharing and Protection Act[53] aimed at increased sharing of information among national security and intelligence agencies and private businesses. This House bill was not supported by President Obama and did not include any mandates for the SEC.[54]

In August 2012, the Senate failed to pass the Cybersecurity Act of 2012.[55] The Senate split largely along party lines, and the Republicans filibustered to defeat the measure.[56] The bill sought to establish standards for computer systems that oversee the nation's infrastructure. In the time before its vote, it was weakened so that certain measures were no longer mandatory but voluntary.[57] The bill also included a mandate for the SEC. Within one year of the bill's passage, the SEC was to evaluate its existing cybersecurity disclosure guidance (including the SEC Guidance) and determine whether any updates were required or whether to issue new interpretative guidance. The SEC was also to be charged for each of the five years following the bill's passage with reporting to Congress regarding: (1) the types of information security risks and related events reported by companies in SEC filings, (2) whether the Staff of the SEC requested additional disclosures regarding cybersecurity matters in company filings, (3) cybersecurity awareness/educational programs sponsored by the SEC or attended by SEC Staff and (4) public actions commenced by the SEC relating to the enforcement of disclosure requirements as related to cybersecurity. In the aftermath of the bill's failed passage, Senator Rockefeller announced that he has written to the nation's largest 500 companies to solicit responses to eight questions "without the filter of beltway lobbyists" regarding each company's cybersecurity policies and practices and views on federal involvement and regulation in this area.[58]

In addition, John Brennan, Assistant to the President for Homeland Security and Counterterrorism, has written a letter to the Chairman of the Committee on Commerce,

Science and Transportation that indicates the President is currently exploring the possibility of an executive order to direct the executive branch departments and agencies to work with private businesses to secure critical pieces of our nation's infrastructure.[59] Such an executive order would not have the impact of legislation passed by Congress but could have similar effects. Senator Rockefeller's letter campaign along with the Administration's statements it is considering the issuance of an executive order clearly show that the topic of cybersecurity will remain in the political spotlight for some time and is a topic that companies must begin to seriously evaluate.

Conclusion

Given the SEC's widespread commenting on this issue, every company, if it has not already done so, should consider, at minimum, the appropriateness of inclusion of a cybersecurity related risk factor in its next annual report on Form 10-K. In an era of ever increasing SEC disclosures, companies should further prepare themselves that the required disclosures surrounding cybersecurity are likely to increase in coming years. While it does not appear that explicit SEC rules or other regulations are on the immediate horizon, the SEC's guidance and commenting process have already effectively created a standard of disclosure.

Notes

1. Available at *http://commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e*.

2. Available at *http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm*.

3. *Supra* note 1.

4. *Id*.

5. The SEC uses the definition of "cybersecurity" from Whatis?com available at http://whatis.techtarget.com/definition/cybersecurity.html.

6. *See supra* note 2.

7. *See* Basic v. Levinson, 485 U.S. 224 (1988) and TSC Industries v. Northway, 426 U.S. 438 (1976).

8. *But see* discussion below under "SEC Comment Letter Trends – Attacks and Breaches" regarding SEC comment letters that indicate that a prior cyber attack or intellectual property security breach should be addressed in risk factors under Item 503(c) of Regulation S-K even if such incident is deemed immaterial (in the individual or aggregate) by a company.

9. *Supra* note 2.

10. *Id*.

11. *Id*.

12. *Id*.

13. See, e.g., Accounting Standards Codification sections 350-40, Internal-use Software, 605-50 Customer Payments and Incentives and 450-20 Loss Contingencies.

14. *Supra* note 2.

15. *See, e.g.,* Staff Comment Letter dated May 3, 2012 to CIT Group Inc., available at *http://www.sec.gov/Archives/edgar/data/1171825/000000000120023091/filename1.pdf;* Staff Comment Letter dated June 28, 2012 to Kellogg Company, available at *http://www.sec.gov/Archives/edgar/data/55067/000000000012033900/filename1.pdf;* Staff Comment Letter dated June 8, 2012 to Wal-Mart Stores, Inc., available at *http://www.sec.gov/Archives/edgar/data/104169/000000000012029999/filename1.pdf;* Staff Comment Letter dated Staff Comment Letter dated April 13, 2012 to Texas Instruments Incorporated, available at *http://www.sec.gov/Archives/edgar/data/97476/000000000012018871/filename1.pdf;* and Staff Comment Letter dated April 12, 2012 to Aon Corporation, available at *http://www.sec.gov/Archives/edgar/data/315293/000000000012018575/filename1.pdf*.

16. *See, e.g.,* Staff Comment Letter dated February 28, 2012 to Facebook Inc., page 4, available at *http://www.sec.gov/Archives/edgar/data/1326801/000000000012014780/filename1.pdf*

17. *See, e.g.,* Staff Comment Letter dated March 19, 2012 to Shinhan Financial Group Co Ltd, available at *http://www.sec.gov/Archives/edgar/data/1263043/000000000012014321/filename1.pdf*.

18. *See, e.g.,* Staff Comment Letter dated March 21, 2012 to Intel Corporation, available at *http://www.sec.gov/Archives/edgar/data/50863/000000000012014462/filename1.pdf*, which requests Intel to "[p]lease tell us what consideration you gave to including disclosure describing [certain] characteristics of your security environment and the implications of such rapid and significant increases in the threats to that environment."

19. Available at *http://www.sec.gov/Archives/edgar/data/874766/000000000012017492/filename1.pdf*.

20. Id.

21. Letter dated April 18, 2012 to the Division of Corporation Finance., available at *http://www.sec.gov/*

Archives/edgar/data/874766/000119312512168405/filename1.htm.

22. Staff Comment Letter dated May 7, 2012 to The Hartford Financial Services Group, Inc., available at *http://www.sec.gov/Archives/edgar/data/874766/000000000012023723/filename1.pdf*.

23. Id.

24. Letter dated May 16, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/874766/000119312512236210/filename1.htm*.

25. Staff Comment Letter dated April 12, 2012 to Aon Corporation, *supra* note 15.

26. Id.

27. Letter dated May 14, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/315293/000110465912036970/filename1.htm*.

28. Staff Comment Letter dated June 4, 2012 to Aon Corporation, available at *http://www.sec.gov/Archives/edgar/data/315293/000000000012028873/filename1.pdf*.

29. Letter dated April 2, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/1365135/000119312512146400/filename1.htm*.

30. Letter dated April 20, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/1365135/000119312512171861/filename1.htm*.

31. Staff Comment Letter dated May 3, 2012 to CIT Group, Inc., *supra* note 15; Letter dated May 15, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/1171825/000089109212002834/filename1.htm;* Staff Comment Letter dated July 6, 2012 to CIT Group, Inc., available at *http://www.sec.gov/Archives/edgar/data/1171825/000000000012035281/filename1.pdf;* and Letter dated July 16, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/1171825/000089109212003915/filename1.htm*.

32. Staff Comment Letter dated July 6, 2012 to CIT Group, Inc. *supra* note 31.

33. *Id*.

34. *Id*.

35. Staff Comment Letter dated May 2, 2012 to Google, Inc., available at *http://www.sec.gov/Archives/edgar/data/1288776/000000000012022687/filename1.pdf*.

36 Staff Comment Letter dated March 12, 2012 to Amazon.com, Inc., available at *http://www.sec.gov/Archives/edgar/data/1018724/000000000012012577/filename1.pdf;* Letter dated April 9, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/1018724/000119312512155627/filename1.htm;* Staff Comment Letter dated April 18, 2012 to Amazon.com, Inc., available at *http://www.sec.gov/Archives/edgar/data/1018724/000000000012019757/filename1.pdf;* and Letter dated May 3, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/1018724/000119312512208583/filename1.htm*.

37. *See* supra note 18 and Letter dated April 18, 2012 to the Division of Corporation Finance, available at http://www.sec.gov/Archives/edgar/data/50863/000005086312000053/filename1.htm.

38. Staff Comment Letter dated May 2, 2012 to Eastman Chemical Company, available at *http://www.sec.gov/Archives/edgar/data/915389/000000000012022648/filename1.pdf;* Letter dated May 16, 2012 to the Division of Corporation Finance (not available on EDGAR); Staff Comment Letter dated May 21, 2012 to Eastman Chemical Company, available at *http://www.sec.gov/Archives/edgar/data/915389/000000000012026294/filename1.pdf;* and Letter dated May 22, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/915389/000119312512243687/filename1.htm*.

39. *Supra* note 37.

40. *Supra* note 38.

41. Staff Comment Letter dated April 13, 2012 to Texas Instruments Incorporated, *supra* note 15, and Letter dated April 27, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/97476/000009747612000024/filename1.htm*.

42. Staff Comment Letter dated March 19, 2012 to Shinhan Financial Group Co., Ltd., *supra* note 17, and Letter dated April 2, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/1263043/000119312512144857/filename1.htm*.

43. *See* Letter dated June 14, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/315293/000110465912043644/filename1.htm*, and *supra notes* 24, 31 and 36.

44. Letter dated July 9, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/77384‰0093041312003900/filename1.htm*.

45. *See supra* notes 19-24.

46. *See supra* note 36.

47. *See* Letter dated May 3, 2012 to the Division of Corporation Finance, *supra* note 36.

48. *See* Staff Comment Letter dated June 28, 2012 to Kellogg Company, *supra* note 15, and Letter dated July 13, 2012 to the Division of Corporation Finance, available at *http://www.sec.gov/Archives/edgar/data/55067/000119312512301697/filename1.htm*.

49. Letter dated July 13, 2012 to the Division of Corporation Finance, *supra* note 48.

50. *Id.*

51. Statement by the Press Secretary on Cybersecurity Legislation Vote on August 2, 2012, available at *http://www.whitehouse.gov/the-press-office/2012/08/02/statement-press-secretary-cybersecurity-legislation-vote*.

52. Id.

53. Available at *http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523eh/pdf/BILLS-112hr3523eh.pdf*.

54. Cybersecurity Bill is Blocked in Senate by G.O.P. Filibuster, *The New York Times*, Michael S. Schmidt, August 2, 2012 (online version).

55. Available at *http://www.gpo.gov/fdsys/pkg/BILLS-112s3414pcs/pdf/BILLS-112s3414pcs.pdf*.

56. *See supra* note 54.

57. *Id.*

58 Letter to International Business Machines dated September 19, 2012 from John D. Rockefeller IV, available at *http://commerce.senate.gov/public/?a=Files.Serve&File_id=396eb5d5-23a4-4488-a67c-d45f62bbf9e5; see also* Senator Presses On Cybersecurity, *The Wall Street Journal*, Siobhan Gorman, September 19, 2012 (online version).

59. Letter from John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, dated September 12, 2012 to the Chairman of the Committee on Commerce, Science & Transportation, available at http://commerce.senate.gov/public/?a=Files.Serve&File_id=f4da0411-6fb3-4f2b-b3d5-0fd6767ec8db.

Six Tips on How to Write an Effective SEC Rulemaking Comment Letter

By Jay Knight

As someone who only recently left working at the SEC, I understand first-hand that writing a comment letter in response to an SEC rule proposal is not an easy task. In most cases, it takes many hours of thoughtful deliberation and hard work to draft a comment letter. Moreover, anyone that spends the amount of time and expense necessary to write a comment letter wants to know that their comments will be understood by the SEC Staff—and that the efforts are delivered with maximum effectiveness.

There is no "model" comment letter that the SEC Staff is looking for. A one sentence comment letter may have the same impact—or even more—on the Staff's ultimate decision about how to craft a rule as a 100-page white paper. However, based on my experience reviewing and summarizing thousands of comment letters while on the SEC Staff, below are some practical tips that you might consider to maximize your comment letter's effectiveness.

1. Read the questions in the release carefully. The Staff takes great care in formulating the questions posed in the release. While some are macro questions, others may give the reader a glimpse into the tough issues that the Staff grappled with when it drafted the proposal. Carefully reading the questions may also help you understand the rationale for parts of the proposal, as sometimes the Staff asks a question on an issue rather than putting it in the proposal. While following along with the questions from the release may help the Staff in pinpointing the issue, there is no requirement that you do so—and you are free to convey your comments in any format that makes presentation flow better.

2. Provide draft rule text. There is nothing that focuses the mind in rulemaking like actually converting comments into draft "reg text." Not only will this exercise fully vet your comments and identify areas of improvement, but it also allows you to see what steps are required for the Staff to implement your ideas. This particular exercise is most helpful in areas where technical details regarding implementation are vital to all parties.

3. Join a group. If you are a company or investor, consider forming a group of like-minded companies or investors. This provides your letter with additional authority by showing others share similar concerns.

4. Check for Commission rulemaking discretion and statutory authority. When the Commission is acting on a statutory directive to write a rule, it is not effective to communicate to the Staff that you disagree with the statute generally. Even if the Staff agrees with you, it has no legal authority to change the statute. It is more productive to provide your comments within the framework given under the statute and to focus your comments on the components of the rule where the SEC has the flexibility to exercise discretion. Moreover, if your comment letter is requesting some type of exemption, be sure to cite the statutory authority the SEC can rely upon to grant your request. Be specific as to how your facts fit within the designated statutory authority. In my experience, commenters requesting an exemption or exception from the rule often fail to fully explore the statutory basis upon which the SEC could grant such exemption or exception. Remember

Jay Knight is an Associate with Bass, Berry & Sims PLC. Prior to this, he was Special Counsel in the Division of Corporation Finance at the SEC.

the SEC is only able to work within the statutory authority given by Congress. To the extent there is exemptive authority—do not assume there always is—be sure to cite this authority and how your request fits within that authority.

5. Comment on economic analysis. If you are able to comment on the SEC's economic analysis or provide your own economic data, please do so! Providing economic data and analysis greatly assists the SEC with fulfilling its mandate to consider the costs and benefits of its rules, especially in light of the high bar set by the *Business Roundtable* court decision, in which the DC Court of Appeals held that the SEC acted arbitrarily and capriciously for having failed to adequately assess the economic effects of its proxy access rule. Even if you are unable to provide quantitative analysis, consider providing a qualitative discussion of the costs and benefits of the rule.

6. Put all your comments in writing. Probably one of the most common obstacles to communicating effectively with the Staff is when the commenter fails to submit its comments in writing. This formal process is usually required for the Staff to rely on the comments under the Administrative Procedures Act, and therefore, the Staff usually requests that commenters submit their comments in writing. Note this applies to meetings with the Staff as well. Thus, to the extent new material is conveyed during a meeting with the Staff, remember to submit the new material in a filed supplemental comment letter.

Once you have written your comment letter, the next step is to file it with the SEC. Certainly, best practice is to submit your comment letter within the designated comment period window (e.g., 30, 60 or 90 days from Federal Register publication). However, the Commission's policy is to consider all comments received up until the time it takes action. Thus, even if you missed the comment period deadline, file it anyway.

After filing your comment letter, you may wish to schedule a 30-45 minute in-person meeting or conference call with the SEC Staff heading the rulemaking project. This is certainly not required or always necessary, but it is not uncommon, and may, in some situations, help the Staff further understand the reasoning behind your comments. The process typically involves reaching out to the Staff member listed in the release as the appropriate contact person.

Although Staff members' schedules are often full, they will typically work hard to accommodate your request for a meeting or conference call. If you choose to schedule a meeting, use it as an opportunity to proactively supplement and explain your comments to the Staff. Do not expect the Staff to lead the meeting on your behalf.

With the SEC still in the throes of Dodd-Frank Act rulemaking, and now in the midst of rulemaking under the JOBS Act, the comment letter process is on the front burner for many desiring to positively impact the SEC's policymaking. To do this, effective communication is required. By incorporating some or all of the tips outlined above, you may increase the chances that your comments are accurately and effectively conveyed to the Staff.

Corporate Internal Investigations: A User Guide for Companies

By Vince Farhat, Vito Costanzo & Stacey Wang

Companies are under increasing pressure to investigate and self-report allegations of corporate misconduct. As government agencies become more aggressive in investigating allegations of corporate fraud and abuse, an unprepared company may unwittingly find itself mired in obstruction of justice charges because initial protective steps were not taken to identify and preserve potential sources of evidence and to establish the independence of the company's decision makers vis-à-vis the alleged misconduct.

This is the second of a three-part series providing companies with a step-by-step guide for planning and conducting sensitive internal investigations into potential wrongdoing. In the July/August 2012 issue of this publication, Part One covered the initial decision of whether to conduct an internal investigation and immediate steps that should be taken to preserve evidence and create an independent investigation. This part addresses how to design and plan internal investigations, including how to define and charter the investigation and document collection and review.

Defining the Scope of the Investigation

Once a company decides to investigate potential wrongdoing, it must define the scope and extent of the internal investigation. This requires companies to balance competing interests. On the one hand, business as usual must go on and companies can ill afford to spend precious resources investigating frivolous and incredible allegations of misconduct. Conversely, credible allegations of misconduct must be investigated and the results documented in a way that will withstand subsequent scrutiny.

One recurring theme is that every case is different; thus, "one size does not fit all" in designing an internal investigation. An internal investigation may be limited to a handful of interviews and the review of a few documents, or it may be a far-reaching effort involving many witnesses around the country (or abroad) and extensive electronically stored information (ESI). Since there is no set playbook, company investigators must document the process; everything is "on the record" during an investigation. The guiding principle in doing so is how outsiders, such as the government, outside auditors and/or the media, will judge the investigation years from now.

One critical factor in defining the scope of the internal investigation is how quickly the company needs the information. The scope of the investigation can depend, in part, on whether the company wants to complete its investigation before the government becomes aware of the issue, whether the government is willing to defer its own investigation to the completion of the company's internal investigation, the timeline for making any mandated self-disclosures to the government, and the need to establish affirmative defenses for the company. The scope of an internal investigation also can be defined by inquiries from government investigators (whether informal or by subpoena), lawsuits or pre-lawsuit demands, and internal compliance reports from employees or customers.

 Vince Farhat and Vito Costanzo are Partners, and Stacey Wang is an Associate, of Holland & Knight LLP. Part Two in a Three-Part Series; Part One was in the July-August 2012 issue.

(i) In line with these considerations, companies should consider the following general factors in assessing the scope of a formal internal investigation.

General Factors in Assessing the Scope of an Internal Investigation
• How did problem surface and who was involved in reporting the issue?
• How much time does the company have to complete the investigation?
• Is the proposed scope of the internal investigation broad enough to determine whether misconduct occurred?
• Is the proposed scope broad enough to permit the company to take remedial action?
• If the results of the investigation were disclosed, is the proposed scope broad enough to satisfy government investigators?
• What steps must be taken to document the investigation and preserve evidence?
• What will it cost to conduct the internal investigation? What steps can be taken to reduce expense without compromising the integrity of the investigation?
• Will the internal investigation disrupt business operations? If so, what steps can be taken to minimize disruption without compromising the investigation?
• Is there a need to maintain confidentiality?

(ii) In defining the scope of the internal investigation, the company must identify critical personnel, documents, and internal procedures that could be implicated in the investigation of the potential misconduct.

The "Who What Where" in Assessing the Scope of an Internal Investigation
• What are the elements of the possible civil claims, regulatory violations, or criminal charges?
• What employee positions are typically associated with the kinds of events or transactions giving rise to the potential misconduct?
• Who are the employees and/or contractors (regardless of their positions) with potential knowledge of the specific issues under investigation?
• Who are the records custodians for company documents of this type?
• Where are the relevant company records? Don't overlook the possibility that, regardless of company policies, the custodians may have relevant information on their personal computing devices.
• What third parties are typically associated with the kinds of events or transactions giving rise to the potential misconduct?

• What customers and/or vendors might have potential knowledge of the specific issues under investigation?
• Where are the above employees, records, third parties located? If any of them are located overseas, consider whether the company needs local counsel and/or local investigators. Foreign laws, such as protections over private information, might be implicated.
• What company procedures are implicated?
• Were company procedures violated? If so, were possible violations documented or recorded?

Chartering the Investigation

After defining the scope of the internal investigation, the company should prepare and formally approve a written document "chartering" the investigation. The Charter can take the form of a resolution from the board of directors or the board audit committee, an engagement letter, or a memorandum issued by senior management or the general counsel. The purpose of the Charter is to:

- *Give company investigators the necessary independence and power to conduct an effective investigation*
- *Clearly identify the scope of investigation*
- *Impose any limitations on the investigators the company deems appropriate*
- *Anticipate means to collect and review documents*
- *Ensure the company preserves evidence even after the investigation is over, i.e., for use in future related actions such as shareholder derivative suits and other related litigation.*

(iii) The Charter should be a "living document" because companies may need to re-evaluate the scope of the investigation based on new information and allow the action plan to develop and evolve as documents are reviewed and witnesses are interviewed. Charters for internal investigations should contain a number of basic elements, described below.

Basic Elements for Internal Investigation Charters
• Specify where appropriate that the investigation is being conducted in anticipation of litigation and for the purpose of obtaining legal advice
• Clearly identify the client, *i.e.* the company, the board of directors, or a board committee
• Describe the scope of the internal investigation
• Identify who is responsible for searching for documents, including Electronically Stored Information (ESI)
• Identify who will be interviewed
• Describe how witness interviews will be conducted
• Explain how third party witnesses will be handled
• Describe who the investigators will report to, *i.e.* entire board, liaison, etc.

(iv) Third parties such as customers and vendors often have important information, but contacting them can endanger the confidentiality of the investigation and might jeopardize the company's relationships with these parties. If company investigators decide to interview third party witnesses, the company should proceed very carefully, since missteps can be viewed by the government as witness tampering or obstruction of justice. Therefore, companies should weigh and document the advantages and risks before deciding to interview third parties, such as:

- Maintaining confidentiality versus obtaining information?
- How will the government view failure to contact the third parties versus the potential perception of witness tampering?
- How to establish/maintain credibility with key constituencies?

Directing the Investigation

As part of chartering the investigation, companies must decide who will direct the internal investigation and assemble the investigation team. As discussed in the first part of this article, red flags of wrongdoing sometimes can be quickly resolved by company personnel. For example, a company's human resources department often has skills and expertise necessary to investigate discrimination or harassment allegations, and a company's audit department often can investigate theft or embezzlement. In these instances, it is strongly advisable to involve in-house counsel to protect attorney-client and work-product privileged information.

(v) Companies may also involve attorneys to direct and plan the internal investigation. It is generally advisable to involve legal counsel where the internal investigation has been triggered by inquiries from government investigators (whether informal or by subpoena), lawsuits, or pre-lawsuit demands. In addition to preserving the attorney-client privilege and attorney work product protection, counsel will bring expertise and experience in conducting investigations and legal advice concerning investigation results.

(vi) A related issue is whether the company should rely on its in-house counsel or retain outside counsel to conduct the investigation. In some cases, in-house counsel may have advised management on the issue under investigation, could be a percipient witness, or may not be familiar with the investigating government agency. Retaining outside counsel adds to the cost of the internal investigation, but may be justified where the company seeks the perception of greater independence and familiarity with the law enforcement agency. Outside counsel also may be necessary where the company needs additional resources for the investigation.

(vii) An internal investigation also may require the assistance of experts such as accountants, engineers, computer forensics, and private investigators. Private investigators should be carefully controlled as they are agents of the company. They should not engage in misrepresentations in order to get information, and the company should not permit investigators to engage in conduct that would be otherwise improper for counsel. The company also should consider using expert retention agreements in conjunction with legal counsel providing legal advice and in anticipation of litigation to as to preserve applicable privileges.

Document / ESI Collection and Review Issues

As a threshold matter, and as discussed in part one, as soon as a company can reasonably anticipate litigation or a government investigation, all routine actions that would result in the modification or destruction of documents or information, including electronically stored information (ESI), that may be relevant to the litigation or

investigation should be suspended. Even if the company does not know particular specifics, the act of enforcing what would ordinarily be a best practice may be viewed as spoliation of relevant evidence or, in a criminal investigation, obstruction of justice. Imaging, or taking a snapshot of, the ESI can provide peace of mind if overriding or modifying data is a concern.

The company should identify and collect an initial relevant universe of hard-copy documents and ESI in the investigative process, not only as part of preserving all evidence, but also to assist in identifying relevant witnesses, framing appropriate topics and questions for interviews, and to refresh witness recollections during the interviews. In some cases, outside counsel may need to retain technology professionals to forensically retrieve, host, and analyze ESI. In-house IT personnel should only be utilized where the company has a sufficiently sophisticated staff trained in issues that may become critical in a subsequent litigation or in a government investigation, such as chain of custody and metadata preservation.

In a perfect world, all paper documents and ESI would be collected and reviewed before witnesses are interviewed. In the real world, one informs the other; company investigators often start the investigation by gathering documents, but they are not compartmentalized steps. Otherwise, it may be possible to miss clues from witnesses of documents in unexpected places.

Although often tedious, document review can be critical to the goal of learning what happened and why. Investigators should make a written record of what they are doing, including an inventory of what documents have been collected and reviewed, and what search terms have been applied, and organize key documents by topic and by individual. These efforts will minimize the need to re-review possibly voluminous documents.

In the age of electronic storage devices, personal digital assistants, and communications that leave an electronic trail (*e.g.*, texts), potential sources of evidence are everywhere. Understanding the company's technology infrastructure and communicating with the information technology department is crucial. After the initial steps of stopping all automated janitorial and overwriting functions and preserving all relevant back up documents, the company may be facing terabytes (or even petabytes) of data. The unwieldy size of potential ESI is an area that cannot be approached with a "paper" mindset and strategy.

Cloud computing has emerged as a popular way to centralize a company's data. In many ways, cloud computing can make data collection in internal investigations easier. For example, the company's IT personnel can very quickly stop automated functions to preserve data. As well, all networked data for relevant custodians can be collected quickly, sometimes without ever alerting the custodian.

However, even with cloud computing, employees may have relevant communications and data on personal devices. The company must ensure that the employees understand that, depending on the sophistication of the technology, even accessing or viewing a file may look like tampering if the metadata cannot confirm that the file has not be modified. In addition, cloud computing platforms typically involve third-party vendors. Such vendors may be served with government subpoenas without notice to the company. The key takeaway is to be aware that whenever data is maintained by a third party, some control is lost.

Generally, the main concern with ESI is the cost of collection, preservation and review. Where the universe of potential ESI is unwieldy, use of predictive coding and other advanced electronic review tools not only save an enormous amount of money and resources as compared to taking a "banker's box" mentality to document review, it may well be the only means to undertake review of massive amounts of data. Until protocols of general acceptance are developed for computer-assisted collection and review, the trend of the best practice in this area is toward reaching agreement wherever possible. That is, where there is opposing counsel, ideally

agreements should be reached, and disputes resolved, before rather than after incurring the expenses for collection and search. The Sedona Principles on the civil side, and the Joint Electronic Technology Working Group's Protocol on the criminal side, have been developed to address best practices in each arena for federal matters, and each continues to be refined. State efforts vary.

As soon as the company realizes that issues regarding ESI will add a layer of complexity, the company should consult outside counsel versed on these best practices, assuming the company does not maintain an in-house ESI group. Not doing so, or going to counsel who insist on approaching the situation with a "paper" mentality is taking a big risk for expensive missteps down the road.

On a last note, special considerations apply when companies are producing documents in response to government subpoenas which are not addressed in this guide. The subpoena will often answer many of the questions the company would otherwise grapple with in the absence of the subpoena's directive on the scope of the investigation.

Part Three *of the series will cover witness interviews, memorializing findings, whether to self-report violations, and handling whistleblowers.*

The Latest: What's on Directors Minds

By Julie Hembrock Daum

As part of our annual corporate governance index, we survey corporate secretaries and general counsel to gain insight into what's on directors' minds and to provide a more complete view of the most pressing governance issues and trends.[1] As part of this survey, we have asked how much focus boards are giving to particular governance topics.

Executive compensation continues to be the top issue; 72 percent of our survey respondents ranked executive pay as the number one governance topic for their board in the past 12 months. "Say on pay" was ranked a top issue by 30 percent of respondents. The board's role in corporate strategy also was a top concern, considered a top issue by 67 percent of respondents. About half of respondents indicated that CEO succession planning and director recruitment are issues requiring the most focus from their boards, significantly higher than in 2008.

Another key focus for boards in 2012 was addressing shareholder concerns or shareholder communications. 29 percent of respondents said shareholder concerns demanded a high degree of focus, while 52 percent said this warranted moderate focus. Boards also are looking internally. 23 percent of respondents said their boards have given a high degree of focus to board leadership structure, while 18 percent said board diversity received a high degree of attention.

Board Composition

Board turnover continues to decline:

- The number of new appointees has dropped by 12 percent over the past five years and by 27 percent over the past 10 years.
- S&P 500 boards elected 291 new directors in the 2012 proxy year. This represents the smallest number of new appointees since 2001.
- The decline in the number of new director appointments in recent years may be attributed to rising retirement ages, fewer voluntary resignations due to lingering effects of economic uncertainty, less urgency to appoint new directors with Sarbanes-Oxley compliance requirements having been fulfilled in the mid-2000s.

First-timers and other corporate executives prove to be attractive director pool:

- 30 percent of the new independent directors are newcomers to outside public-company board service.
- One-quarter of new independent directors are active CEOs, COOs, chairmen, presidents and vice chairmen, down from 41 percent a decade ago.
- As active CEOs take on fewer boards, more companies are turning toward other corporate executives, both active and retired, to fill the boardroom. Division/subsidiary presidents and other line and functional leaders now make up 22 percent of all new directors, versus seven percent a decade ago.
- The share of new directors who are retired top executives fell slightly in the past year, from 19 percent in 2011 to 16 percent today. Yet, ten years ago, this group accounted for only 11 percent of the total.
- Demand for director candidates with financial backgrounds saw a small uptick in the past year; 22 percent of new appointees have banking, finance, investment or accounting credentials, compared with 18 percent in 2011 and 19 percent five years ago.

 Julie Hembrock Daum is Co-Leader of the North American Board & CEO Practice of Spencer Stuart.

- Overall, 62 percent of new independent directors are active executives or professionals and 38 percent are retired. In 2007, the split was 71 percent and 29 percent respectively.

- One-third of new directors bring global experience, as defined by working in an international location, while 8 percent of new directors have some working experience in the government or military.

- 74 percent are men and 26 percent are women, versus 84 percent and 16 percent 10 years ago.

- Of the new women directors, 18 percent are current/former CEOs and more than one-third are current or former corporate executives. Among men, about half of the incoming directors are current/former CEOs and 18 percent are division/subsidiary presidents or line/functional leaders.

Average board size unchanged, but fewer large boards:

- The average board size has changed little in the past 10 years. On average, S&P 500 boards have 10.7 members today, versus 10.8 five years ago and 10.9 in 2002. However, the average does mask a general move to smaller boards. Today, 86 percent of boards have 12 or fewer members, compared with 68 percent of boards a decade ago.

- CME Group continues to top the list of largest boards with 28 members. BlackRock has the next largest board, with 17directors.

- The smallest board—Microchip Technology—has just five directors, while seven others have six.

Percentage of independent directors stabilizing:

- Overall, independent directors make up 84 percent of all board members, consistent with the past two years. The ratio of independent to non-independent directors is 5.3 to 1 versus 3.8 to 1 a decade ago.

- The CEO is the only non-independent director on 59 percent of S&P 500 boards, a slight increase from 57 percent in 2011. This number has nearly doubled in the past decade, from 31 percent in 2002 and 43 percent in 2007.

Annual director elections and majority voting becoming the standard:

- 83 percent of boards now have declassified structures, a notable increase from 76 percent in 2011. The share of boards with one-year director terms has more than doubled from 40 percent a decade ago.

- Another area where governance practice has evolved is in the adoption of policies requiring directors who fail to secure a majority vote to offer their resignation. 84 percent of boards today now have such policies, up from 79 percent in 2011 and 56 percent in 2008, the first year we tracked the data.

- While these policies are becoming commonplace, boards still retain the discretion to accept or decline a director's resignation following his or her failure to receive a majority vote.

Boards continue to establish resignation policies for directors and CEOs:

- The corporate governance guidelines for 85 percent of boards contain a policy whereby directors who experience changes in job circumstances or responsibilities must notify the chairman and/or the nominating committee and offer their resignation.

- 34 percent of boards require the CEO to submit his or her resignation from the board when the CEO's employment with the company ends. In all cases, however, boards retain the discretion to accept or decline the resignation.

Restrictions on other corporate directorships more common:

- Given the time and commitment required for effective board service, 74 percent of S&P

500 companies now limit other corporate directorships for their board members, the same as last year but significantly more than 55 percent five years ago. Some companies limit the number of additional boards for all directors, while others do so only for directors fully employed by public companies.

- Of the 127 boards that do not specify any limits, 108 (85 percent) ask that directors notify the chairman in advance of accepting an invitation to join another company board and/or encourage directors to "reasonably limit" their other board service.

- Of the 286 boards that impose a numerical limit for all directors, 5 percent cap additional directorships at two boards, 30 percent at three boards, 41 percent at four boards and 24 percent at five or more. None limit other directorships to one.

- 76 boards place tighter restrictions on directors who are fully employed executives or CEOs of public companies — most often this cap is set at two outside boards.

- 45 percent of S&P 500 boards place limits on the number of other audit committee memberships their own audit committee members may serve, compared with 18 percent in 2007. Most of these put the maximum at two additional memberships.

Added Perspective

- The composition of the board has continued to evolve as boards respond to new governance requirements and changing business demands. As a result, we track the backgrounds of new directors and survey corporate secretaries about the expertise and backgrounds that are most in demand.

- Active CEOs and COOs are the highest in demand, with 58 percent of respondents saying they sought active executives for board seats. Executives retired from these roles also are in demand, although not to the same degree. 35 percent of respondents said their boards seek to recruit retired CEOs and COOs. Although demand is high for active and retired senior executives, the pool of candidates who fit these profiles is limited. They represented 25 percent and 16 percent of all new directors in 2012, respectively.

- Another priority, according to our survey, is recruiting minority and women directors. Roughly half of respondents said they are looking for minority directors, but only 12 percent of the new independent directors in 2012 come from diverse ethnic backgrounds. 52 percent of respondents said their board would like to add female directors, while women represented 26 percent of new directors in 2012.

- Interest in adding international expertise increased from 39 percent in 2011 to 46 percent in 2012. Only nine percent of new independent directors in 2012 are not US nationals, but one-third have at least some international work experience.

- Financial and industry experience continue to be desired backgrounds for new directors. More than one-quarter of respondents said their boards are looking for directors with regulatory or governance expertise, and nearly the same number indicated that risk expertise is a priority.

CEO Succession Planning

- Most survey respondents (71 percent) report having succession plans both for emergency or short-term transition needs and for long-term succession. 21 percent have plans for emergency situations only, while 3 percent said they only have a long-term succession plan, five percent said they have neither.

- Nearly two-thirds of the boards (65 percent) of responding companies make CEO succession a formal board agenda item annually, and one-third discuss succession more than once a year. 2 percent address success less than once a year.

- Just over half indicated that the full board has primary responsibility for CEO succession planning (other than the CEO himself or herself). The nominating/governance committee has primary responsibility at 22 percent of responding companies, and the compensation committee at 16 percent.

- Boards look to the CEO to play various roles in the process, most often; the CEO evaluates internal candidates and reports back to the board. The CEO drives the succession process at 19 percent of responding companies and serves as counsel to the board/committee at 26 percent of the companies.

- Nearly three-quarters of boards (72 percent) actively involve human resources in CEO succession planning.

- Just under half of respondents (49 percent) said they have a formal process for reviewing internal succession candidates. Of those, 55 percent benchmark internal candidates against external candidates.

- To help prepare them for the CEO role, internal candidates make presentations to the board and regularly attend board meetings. Nearly 30 percent of respondents said internal candidates are encouraged to serve on outside boards as part of their preparation.

Evaluating Internal Candidates

- Most commonly, directors get to know internal candidates through formal presentations to the board (97 percent) and company-sponsored dinners and events (85 percent). 56 percent said directors get a chance to observe executives during company site visits and 19 percent set up individual meetings between board members and candidates.

Note

1. The *Spencer Stuart Board Index* is based on our analysis of the most recent proxy reports from the S&P 500, plus an extensive supplemental survey, drawing on the latest proxy statements from 486 companies filed between May 15, 2011 and May 15, 2012, and responses from 101 companies to our governance survey conducted in the second quarter of 2011. There may be a plus or minus one percent (1 percent) margin of error due to rounding throughout the report. Survey respondents are typically corporate secretaries, general counsel or chief governance officers. Proxy and survey data have been supplemented by information compiled in Spencer Stuart's proprietary database.

the Corporate Governance Advisor

ASPEN PUBLISHERS

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

Wolters Kluwer
Law & Business

Aspen Publishers
The Corporate Governance Advisor
Distribution Center
7201 McKinney Circle
Frederick, MD 21704

TIMELY REPORT

Please Expedite

November/December 9900529035