the Corporate Governance Advisor

March/April 2017 • Volume 25, Number 2

CYBERSECURITY

Top Cybersecurity Concerns for Every Director

By John Reed Stark

Every board now knows its company will fall victim to a cyber-attack, and even worse, that the board of directors will need to clean up the mess and superintend the fallout.

The threat seems even more ominous of late. Recently, two senior cybersecurity officials went so far as to say that the world should brace itself for more physically destructive hacks, warning that a more dangerous era of hacking was already upon us.

Paul Chichester, the director of operations at Britain's new National Cyber Security Center, told attendees at an event hosted by British defense think tank the Royal United Services Institute (RUSI) that electronic intrusions were on their way to becoming more "destructive, disruptive and coercive." "That will be our future," he told the crowd. Chichester was seconded by Air Force Lt. Gen. James K. McLaughlin, deputy commander at U.S. Cyber Command, who similarly stated that infrastructure-wrecking attacks were being seen "right now in the environment."

Continued on page 2

Wolters Kluwer

CONTENTS

Yet cyber-attacks can be extraordinarily complicated and, once identified, demand a host of costly responses. These include digital forensic preservation and investigation, fulfillment of state and federal compliance obligations, potential litigation, engagement with law enforcement, the provision of credit monitoring, crisis management, a communications plan—and the list goes on. Additionally, constituencies that may require notice, briefings, and other information include customers, partners, employees, affiliates, insurance carriers, and a range of other interested parties.

And besides the more predictable workflow, a company is exposed to other, even more intangible costs as well, including temporary, or even, permanent reputational and brand damage; loss of productivity; extended management drag; and a negative impact on employee morale and overall business performance.

What is the role of a board of directors amid all of this complex and bet-the-company workflow? Corporate directors clearly have a fiduciary duty to understand and oversee cybersecurity, but there is no need for board members (many of whom have limited IT experience) to panic.

This four-part series discusses cybersecurity considerations that provide a solid bedrock of inquiry for corporate directors who want to take their cybersecurity oversight and supervision responsibilities seriously. These recommendations provide the requisite strategical framework for boards of directors to engage in an intelligent, thoughtful, and appropriate supervision of a company's cybersecurity risks.

This first article of this series discusses cybersecurity considerations relating to the governance, practices, policies, and procedures of a strong cybersecurity program. The second article pertains to cybersecurity areas that involve people, while the third article of the series discusses the more technical areas mandating meaningful board oversight. The final part of the series discusses the board's oversight responsibilities with encryption and data mapping—and also provides some thoughts on this series overall, together with some final thoughts.

By using these concerns as a guide, boards of directors can not only become more preemptive in evaluating cybersecurity risk exposure but they can also successfully elevate cybersecurity from an ancillary IT concern to a core enterprise-wide risk management item, at the top of a board's oversight agenda.

Cybersecurity Governance Generally

The cybersecurity policies, practices, and procedures in place at any company provide a critical indicator of cybersecurity wellness and should be one of the primary focuses of any cybersecurity due diligence effort.

Threat landscapes, activists, random hackers, and state-sponsored actors constantly evolve, refining their techniques, altering their motivations, and shifting their resources, so the best approach for a cybersecurity due-diligence team is to avoid checklists and conduct cybersecurity due diligence in a thoughtful and holistic manner. Effective cybersecurity due diligence carefully considers changing threat actors, advance network telemetrics, and emerging attack vectors.

This article outlines the various policies, practices, and procedures involved in the current board oversight paradigm, organizing data points into broad categories to facilitate the most effective and efficient approach.

Incident Response Plan

Having a cyber-attack incident response plan is a notion that has been preached over and over again to every company (public or private), and that is an important starting point for analysis during any cybersecurity due-diligence exercise. Every company should have, available for review, a current documented incident response plan that is approved by senior management and is reviewed and re-approved at least annually.

When contemplating cybersecurity, most companies allocate significant resources to fortifying their networks and to denying access to cyber-attackers. However, it is now a cliché, well-founded in reality, that data breaches are inevitable. As cybersecurity experts have noted, "There's a saying in the cybersecurity industry that there are two types of businesses today: Those that have been breached and know it and those that have been breached and just don't know it."

Along those lines, just as a company has a fire evacuation plan for a building, it should have a plan in place to manage data breaches, an art form less about security science and more akin to "incident response." At the least, an incident response plan specifies the:

- Members, titles, and contact details of the response team responsible for each of the functions of the plan (management, IT, information security, human resources, compliance, and marketing);
- Communication lines in the event of a cyber-attack;
- Notification protocols and priorities (including law enforcement, regulators, customers, joint venture partners, vendors, and anyone else who might require, or contractually be entitled to, notice);
- Documentation and logging plans in the event of a breach;
- Contact list of relevant outside parties such as outside counsel (who specializes in data breach response), outside digital forensics experts, local law enforcement agents, public relations firms, and relevant financial firms (including the company's bank and insurer);
- Company employees who have authority to speak and make certain decisions about the investigation;
- Cyber insurance information;
- Containment, remediation, recovery, training, and testing plans; and
- Nature and location of any data that is covered by other legal obligations, like medical records under HIPAA, financial records under the Graham Leach Bliley Safeguards Rule or specific, contractually created, data protection/breach notification requirements.

Company executive management should understand its current incident response plans; when the plan was last updated (and how often); who prepared the plan; who approved the plan; and the plan's general approach and principles. There should also exist an accurate and current network topology diagram that is adequately documented and periodically re-assessed and revised as internal systems and external factors change.

Company executives should also avoid using templates for incident response plans. Although templates can serve as a decent starting point, no two companies are identical and all have different business processes, network infrastructures, and types of data-sets. Along these lines, NIST, the National Institute of Standards and Technology, has published a Computer Security Incident Response Guide to help companies develop appropriate policies and procedures and provide a useful reference for companies when meeting with IT department heads. The abstract for the NIST Guide states:

> Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate

response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.

Boards should carefully review incident response plans, including whether evidence of any data security incident is collected and retained so as to be presentable in court, to regulators, to customers, to partners, and to any other interested constituency. Boards should also carefully probe how the incident response plan is tested, what remediation occurs after testing, and how often the plan is reviewed and revised.

Business Continuity Plan

The critical importance of a business continuity plan in the event of a natural disaster is widely recognized and accepted. Yet, too often, such plans are not evaluated in the context of assessing cybersecurity risks.

Even when an organization's IT cybersecurity response fully aligns to IT best practices, there are benefits in integrating IT's response into the existing business continuity structure, rather than having two separate response models. Business continuity is particularly important when dealing with the impact of, and recovery from, a cyber-attack. Speed and agility are key enablers in cyber-incident response, and business continuity enables nimble, rapid response, limiting financial and reputational impact on the enterprise.

For instance, a rising threat to companies is ransomware, a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. The Federal Bureau of Investigation (FBI) notes, "Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted recently by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them." Individuals and organizations are discouraged from paying the ransom, as this does not guarantee access will be restored. The FBI warns:

> The FBI doesn't support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee an organization that it will get its data back—we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals.

A powerful data-recovery plan, which is properly integrated with an incident response plan, contemplates the threat of ransomware and plans for data recovery (perhaps with specialized back-up data systems). As ransomware techniques and malware continue to evolve, the FBI recommends that organizations in particular should focus on two main areas:

- Prevention efforts—both in terms of awareness training for employees and robust technical prevention controls; and
- The creation of a solid business continuity plan in the event of a ransomware attack.

Boards should determine whether a company has properly evaluated the effectiveness of its business continuity plan in the context of a cyber-attack, and if the business continuity plan should be reconsidered and refreshed with these additional considerations in mind. Boards also should probe:

- Whether the policy is regularly reviewed to determine whether the controls are operating as intended;
- How often changes and enhancements to the policy are necessary;

- Whether (and how often) a company tests its business continuity plan from both a technical and operational perspective;
- Whether the company has established a dedicated location to retain backup copies of all critical data, and whether off-site data is encrypted and stored securely;
- Whether employees clearly understand business continuity procedures; and
- Whether a company initiates training and maintains established documentation for its business continuity plan.

Boards also should investigate whether a recovery plan is correlated with business needs, with designated recovery point and recovery time objectives, for situations (such as ransomware) when critical or other necessary systems become unavailable.

IT Security Budgeting

C-suite executives need to view cybersecurity as their company's immune system, which needs flexible funding and talent to avoid the severe losses commonly associated with cyber-attacks. Most budgeting at companies is conducted annually and planned carefully and thoughtfully before the beginning of a company's fiscal year, which makes good sense and is also a sign of a well-run financial team. Yet cybersecurity budgetary priorities can shift quickly and are not well-suited to the standard budgetary planning regimen. A one-year budgetary cycle might not be swift or agile enough to manage rapidly emerging cyber-threats, and an overly rigid, lengthy, cumbersome, or otherwise bureaucratic approach toward cybersecurity can create cybersecurity challenges at even the well-run companies.

Boards should understand how cybersecurity budgeting works; how emergency items are identified and funded; and whether the budget appropriately provides for contingencies in the event of a cyber-attack or cybersecurity need.

Drills and Table-Top Exercises

Table-top exercises enable organizations to analyze potential emergency situations in an informal environment and are designed to foster constructive discussions among participants as they examine existing operational plans and determine where they can make improvements. Such exercises are a natural fit for information and physical security because they provide a forum for planning, preparation, and coordination of resources during any kind of attack.

Most cybersecurity firms and pen-testing firms offer some form of table-top exercise program, which should, in order to be successful: involve detailed preparation; include multiple parties throughout the company; leverage resources from within the company industry and government; and be timely and realistic. Companies (after consulting with counsel) should also reach out to law enforcement agencies such as FBI and request that a federal agent participate in the table-top drill or exercise. The FBI supports participation and collaboration with U.S. companies, and can provide valuable insight throughout the drill.

Boards should review carefully the efficacy, timeliness, frequency, and overall results of a company's table-top drill and even more importantly, analyze what remediation and other corrective measures were taken after those exercises.

Cyber Insurance

A near certainty for public and private corporations is that, at some point, they will be subject to a cyber-attack. And what is indisputable is that cyber-attacks are almost always extraordinarily complicated and will require a host of costly responses. So it seems that for today's risk-averse companies, the best way to gain insight into the question of cyber insurance is not only by understanding the growing and complicated hazard of cyber-attacks, but also by obtaining a stand-alone cyber insurance policy that contemplates carefully the workflow that typically occurs during their aftermath.

Traditionally, purchasing insurance coverage begins with a policy review, a risk breakdown, and a range of other risk-related analytics. However, when contemplating a cyber insurance policy, companies should initiate more of a "reverse-gap" approach toward that calculus, analyzing and scrutinizing the typical cyber-incident response workflow that follows most cyber-attacks.

By analyzing and revisiting the realities and economics of this workflow, a company can then collaborate with its insurance sales representatives and originators to allocate risk responsibly and determine, before any cyber-attack occurs, which workflow costs will trigger coverage; which workflow costs will be outside of coverage; and which workflow costs might be uninsurable.

It is also crucial that companies conduct the necessary due diligence to be sure that their cyber insurance carrier has a good claims-paying and claims-handling history and has a proven record of rapid and supportive response. When a cyber-attack occurs, too often there are doubts as to coverage, which can affect incident response.

Cyber insurance policies also can differ dramatically in their goals and objectives. For example, some policies are designed to cover HIPAA and PCI violations, as well as other regulatory noncompliance, while other policies are geared more for direct financial losses due to wire transfer fraud. For instance, if a company manages trust accounts on behalf of customers, the company likely will require insurance coverage for direct cash losses in the event of a network intrusion that results in the unlawful transfer of funds.

Cyber insurance policy premiums are "not one size fits all," as premiums are factored on a company's industry, services, data risks and exposures, computer and network security, privacy policies and procedures, and annual gross revenue. At present, there are 70 or so insurance carriers writing cyber insurance policies, and nearly all of those policies are issued on a surplus lines basis with potentially significant differences in policy wording from one cyber policy to the next.

Boards should ask whether their senior executives have considered reviewing actual cyber-attacks, analyzing and scrutinizing the typical cyber-incident response workflow and "workstreams" that follow most cyber-attacks. By analyzing and revisiting the realities and economics of these workstreams, a company can then collaborate with their insurance sales representatives and originators to allocate risk responsibly and determine, before any cyber-attack occurs, which workstream costs will trigger coverage; which workstream costs will be outside of coverage; and which workstream costs might be uninsurable.

It is also crucial that boards confirm that the cyber insurance carrier their company uses has a good claims-paying and claims-handling history and has a proven history of rapid and supportive response. When a cyber-attack occurs, too often there are doubts as to coverage, which can impact incident response.

Whatever the type of insurance held by a company, an insurance claim will undoubtedly follow, and insurance adjusters will scrutinize all invoices pertaining to the response to the cyber-attack and the overall cybersecurity of the company, and will require briefings and documentation regarding all investigative efforts. For maximum objectivity, credibility, and defensibility, rather than the company itself, boards should make sure that the independent digital forensic firm investigating the breach, at the direction of counsel, should lead any briefings with insurance carriers.

Boards also should make sure that during any sort of data breach response, a professional on the incident response team, preferably counsel, maintains carefully written documentation of all efforts of the response. This will help later on when gathering the "documentation package" to present to an inquisitive insurance adjuster when seeking an insurance reimbursement for the costs of the breach.

Third Party Cybersecurity Due Diligence

Outsourcing of services (such as IT, payroll, accounting, pension, and other financial services), which typically involve the transfer of, or allowing access to, personally identifiable information (PII) from a company to its vendor, has become increasingly common for today's corporations.

Given that cyber-attackers will often traverse across a company's network and into the networks of its vendors or vice versa, cyber-attacks can often result in disputes as to the culpability for an attack. As a result, in most data breach scenarios, vendors and companies can end up pointing the finger at one another for their respective cybersecurity failures.

Thus, boards should be concerned whether any third-party vendor has access to a company's networks, customer data, or other sensitive information—or whether there exists any sort of other cybersecurity risk of the outsourced function.

In addition, boards should understand how the company incorporates requirements relating to cybersecurity risk into its contracts with vendors, and that these requirements may trigger notification responsibilities. In the event of a data breach, corporate vendors will want to know all relevant facts relating to the cyber-attack, especially:

- Whether their data has potentially been compromised;
- Whether services will experience any disruption;
- The nature of remediation efforts;
- Whether there are any official or unofficial findings of any investigation; or
- Whether there is any other information that can impact their operations or reputation.

Vendors may also request images of malware and indicators of compromise (IOCs) or to visit and inspect the company with its own investigation team. Vendors may ask for weekly or even daily briefings and may demand attestations in writing with respect to any findings pertaining to their data. Some customers may also have contractual language establishing their rights when a cyber-attack occurs, which can range from notification, to on-site inspections, to the option of an independent risk and security assessment of the victim company (at the victim company's, and not the customer's, expense).

Moreover, if third-party vendors conduct remote maintenance of a company's networks and devices, in the event of a cyber-attack, the company may want to confirm it can obtain copies of any relevant logs, as well as access the third-party system to scan for IOCs.

Boards should probe the practices and procedures with respect to the cybersecurity of third-party vendors. Boards should also ask about the company's information security procedures (including training) concerning third-party vendors authorized to access a company's network.

BYOD

Many companies allow their employees to "bring your own devices" (BYOD), especially given customer expectations of 24–7 communication lines, work-at-home situations, and the travel demands on corporate employees. Despite all of the security risks BYOD poses to an IT environment, the trend of companies embracing BYOD in the workplace continues to grow at a rapid pace. In fact, in 2013, more than six out of 10 small and medium-sized businesses had a BYOD policy. By 2020, it is estimated that 85 percent of businesses will have some kind of BYOD program in place.

The security risks surrounding BYOD are obvious: loss of control and visibility of the enterprise data that is being transmitted, stored, and processed on a personal device; malware infiltration of the device; potential data leakage

or disclosure of enterprise data on a device; physical loss or theft of the device; and devices with compromised integrity, such as smartphones that have been rooted or jail-broken by their owners.

Boards should make sure that a company has total control over all BYOD devices, including all applications contained on the devices, as well as the ability to remotely wipe all data from devices. Boards also should focus on whether a company has put into operation robust mobile device management platforms that support containerization of business and personal data, enhanced security controls, encryption key escrow, and tracking and management of laptops, tablets, mobile phones, and other mobile devices.

The Cloud

Cloud storage has many potential advantages for companies, including cost savings, scalability, increased mobility and easier collaboration. However, when a company stores critical or confidential information in the cloud, that information is essentially stored off-site, possibly in another country, and companies should make sure their respective companies are using cloud providers that can reasonably protect and provide assurances on overall data security.

Along the same lines, cloud-based file-sharing services, such as Dropbox, Google Drive, Box, and others, are another way confidential information leaks out of a company. Such cloud services often are used through personal accounts, despite many large companies prohibiting, as a matter of policy, the use of such services for these purposes. Some companies also block access to such services from the company's desktop computers with effective security controls, while other companies are less sophisticated or simply resist the notion of becoming the automated "data nanny" for their employees.

Given the increased adoption of cloud-based services by enterprises of every kind, cyber-attacks on cloud environments have reached almost the same level as attacks on traditional IT. Boards should probe a company's cloud-related practices. Questioning should include especially an assessment of any enterprise-grade security systems and analytics, a determination of the attack vectors, and a review of data security measures.

Important questions include:

- Whether the cloud data is encrypted (in transition and in motion);
- Who holds the encryption keys for cloud data;
- Whether the cloud data is subject to search and seizure (both domestically and internationally);
- The nature of data protections used by the cloud firm;
- How transparent the cloud providers' own security systems are;
- What access can the company get to the cloud provider's data center and personnel to ensure the security system is in place and functioning and make sure it can make a risk assessment and design a response plan;
- Whether company customers have given approval for cloud storage of their data;
- What the cloud servicers' responsibilities are to update their security systems as technology and cyber-attack sophistication evolves;
- How the cloud providers continuously monitor, detect, and respond to security incidents;
- What cloud logging exists and how long logs are maintained;
- How and when cloud data is destroyed;
- Whether cloud data could be subject to a litigation hold and what technologies allow for the cloud data's perusal;

- What auditing is permitted of the security capabilities of the cloud company;
- What regulatory and privacy requirements for PII, personal financial information, personal healthcare information, or other customer data are triggered by the cloud data;
- Whether the cloud firm and the company have any indemnification agreements or evidence of cyber insurance;
- Whether the company's insurance policies cover losses from activities undertaken by the cloud service providers in the event of a cyber-attack;
- What types of pen testing are undertaken by the cloud firm; and
- What the specific details and efficacy of security policies and procedures of the cloud firm are.

Boards also should confirm that a company has a comprehensive means to prevent sensitive data from being uploaded for inappropriate sharing, and the requisite visibility and access to detect anomalies, conduct further investigation, and take quick and decisive remedial action. Along these lines, questions should cover technologies used to prevent the unauthorized use of cloud applications by employees; internal controls regarding any cloud applications used by employees; an incident response plan for handling an attack on any cloud application; and employee training concerning use of cloud applications.

Staying Current

Not all companies face the same cybersecurity risks. There is no one-size-fits-all approach. Companies that house and maintain large amounts of critical information and data need to tailor any defense, mitigation, and response plans accordingly. By taking steps to ensure that information flow about data breaches within the industry and the latest intelligence about rising threats are considered by IT management on an ongoing basis, companies can stay current on the latest threats and prepare accordingly. Preparedness is the key.

Boards should determine what steps a company has undertaken in the realm of security science to stay current about the latest cybersecurity intrusion *modus operandi* and data breach trends. Staying current should be an active aspect of cybersecurity defenses and a required (and encouraged) goal for all IT and other cybersecurity employees. The C-suite also should be briefed routinely about current threats, together with practices, policies, and procedures for addressing suddenly emerging cybersecurity threats.

Lessons Learned from Prior Attacks

When a company experiences a cyber-attack, aside from the cyber-attack's investigation and remediation, a company should also engage in a bona fide review after the fact—and organize and document the lessons learned.

For example, DOS (Denial of Service) or DDOS (Distributed Denial of Service) attacks continue to pose a serious threat to most companies, especially those with an active online commerce component to their operations—and should always be an important Board concern. Boards should have an understanding of how many DOS/DDOS attacks the company has experienced, the specific actions a company is taking to deter DOS/DDOS attacks, and what the company has learned from prior DOS/DDOS attempts.

FAQs: Majority Voting for Directors

By the Council of Institutional Investors

What Is Majority Voting for Directors?

The Council of Institutional Investors (CII) considers companies to have majority voting when they require nominees to receive more "for" votes than "against" votes to be elected (or re-elected) to the board. Majority voting helps make board members responsive to the people they represent.

There is no standard definition of majority voting across the market. A company's definition of majority voting does not necessarily include permitting shareholders to vote against nominees, and it almost never includes relinquishing the board's authority to indefinitely retain majority-opposed directors.

There are just two ways to elect directors: by a plurality of votes cast and by a majority of votes cast. Policies and provisions determining what happens after the vote significantly affect how those vote requirements impact board composition. CII therefore discusses in this FAQ four discrete iterations of director election regimes:

- Strict plurality
- "Plurality plus" board-rejectable resignation
- Majority voting with board-rejectable resignation
- Consequential majority voting

Which Approach Do Most Companies Take?

Although nearly 90 percent of S&P 500 companies use majority voting in some form, just 29 percent of Russell 2000 companies use a majority vote standard in uncontested elections, according to FactSet. Most mid-cap and small-cap companies elect directors (when there is no contest for seats) by plurality vote. Most overseas markets use a majority vote standard in some form. Only a handful of US companies, such as Microsoft, provide for consequential majority voting.

What Is Plurality Voting?

With plurality voting, the nominees who receive the most "for" votes are elected to the

the Corporate Governance advisor

The ***CORPORATE GOVERNANCE ADVISOR*** (ISSN 1067-6171) is published bimonthly by Wolters Kluwer at 76 Ninth Avenue, New York, NY 10011. Subscription rate, $895 for one year. POSTMASTER: Send address changes to *THE CORPORATE GOVERNANCE ADVISOR,* Wolters Kluwer, 7201 McKinney Circle, Frederick, MD 21704. Send editorial correspondence to Wolters Kluwer, 76 Ninth Avenue, New York, NY 10011. To subscribe, call 1-800-638-8437. For Customer service, call 1-800-234-1660.

board until all board seats are filled. In an uncontested election, in which the number of nominees and available board seats are equal, every nominee is elected upon receiving just one "for" vote.

A plurality standard is the best approach to contested elections and is appropriate for the small number of US companies that permit cumulative voting. But a plurality standard is not appropriate for uncontested elections with no cumulative voting.

Almost all companies with plurality voting give shareholders an option on the ballot to "withhold" their vote. Withholding a vote allows shareholders to communicate their dissatisfaction with a given nominee, but it has no legal effect on the outcome of the election. Withholding a vote is fundamentally equivalent to an abstention, although as a practical matter, many interpret it as a non-binding "against." CII is concerned that some investors may believe incorrectly that a "withhold" option has legal significance different from an abstention.

Plurality voting in uncontested elections makes directors more accountable to each other than to the shareholders they represent. It's a "rubber stamp" process that entrenches boards and, in rare instances, elects directors who lack the confidence of shareholders representing a majority.

What Is 'Plurality Plus'?

In response to growing investor concerns about the lack of accountability inherent in plurality voting, since 2004 some companies have modified their plurality standard, either through non-binding policies or bylaw amendments, to require that a majority-opposed director (for whom "withhold" votes exceed "for" votes) must tender her resignation to the board. However, at "plurality plus" companies, a nominee who fails to receive majority support is legally elected for another term, subject to board acceptance of the individual's resignation. Boards in the large majority of cases have rejected resignations in this situation.

CII views plurality plus as a step in the right direction, but not the best way to elect uncontested directors. Plurality plus preserves board control regardless of the voting results. CII encourages plurality companies to skip "plurality plus" and adopt consequential majority voting.

What Is Majority Voting with Board-Rejectable Resignation?

With majority voting, uncontested nominees must receive more "for" votes than "against" votes to be elected. Importantly, this standard properly denies majority-opposed nominees the honor of being legally elected to the board. However, almost all companies with majority voting couple that standard with a resignation requirement for defeated directors. Under the terms of the requirement, the board retains ultimate control over whether the individual departs from the board or stays.

This is the form of majority voting found at most S&P 500 companies. Given its widespread prevalence, CII currently accepts this form of majority voting if the company already has it in place, and the board has a good-faith commitment to replace unelected directors within a reasonable period of time. Yet the core problem persists; uncontested director elections remain functionally symbolic. CII therefore recognizes consequential majority voting as best practice.

Shareholders have other non-binding mechanisms to express their collective views, including shareholder proposals and non-binding "say-on-pay" votes. Director voting, the basis for board legitimacy, should be binding. Plurality-plus and majority vote standards that permit the board to reject a resignation or immediately reappoint the rejected director leave the actual decision on a board member's continued service in the hands of the board. In the rare cases in which directors are rejected in uncontested votes, it is not clear that the board, which tends to be put on the defensive by votes against any of its members, should be trusted to make this decision, except for a reasonable holdover period to arrange for board change.

What Is Consequential Majority Voting?

Consequential majority voting requires an uncontested nominee to receive more "for" votes than "against" votes in order to be elected and establishes a reasonable point at which an unelected director may no longer serve on the board. It is the only approach that places ultimate authority in the hands of the company's owners. In this regard, it is the only approach with "teeth."

Some investors oppose this approach because in certain situations, shareholders oppose directors based on a policy matter, and in the view of these investors it is acceptable for the individual to continue on the board if the policy matter is resolved or meaningfully addressed. In some cases, this even extends to the director's behavior. For example, some incumbent directors are rejected due to poor attendance at board meetings, and shareholders can be amenable to their continued service with a pledge by the individual to improve attendance.

For sample bylaw language providing for consequential majority voting, please refer to Appendix 1, which provides both a Delaware-compliant example and a Model Business Corporation Act (MBCA) version.

Does a Majority Standard (Whether Traditional or 'Consequential') Create the Potential for an Abrupt Board Vacancy upon a Director's Defeat?

In order to be workable, any majority vote requirement must be coupled with some form of "holdover" provision ensuring reasonable accommodation for a smooth transition in the event of a director's defeat. The purpose of a holdover provision is twofold: to safeguard against a hasty recruitment process for a suitable replacement, and to maintain compliance with the company's governing documents, contractual agreements, exchange listing standards, and regulatory requirements throughout the transition period. Holdover provisions typically allow 90 days for the transition, and CII believes a window of up to 180 days is reasonable in certain circumstances.

Is Consequential Majority Voting Permissible under State Law?

Yes. Section 141 of Delaware General Corporation Law provides that each director shall hold office until such director's successor is elected and qualified or until such director's earlier resignation. A 2006 amendment to Section 141 clarified that "a resignation is effective when the resignation is delivered unless the resignation specifies a later effective date or an effective date determined upon the happening of an event or events [including failure to obtain a majority of votes cast]. A resignation which is conditioned upon the director failing to receive a specified vote for reelection as a director may provide that it is irrevocable."

Although many Delaware companies since 2006 have amended their bylaws to adopt a majority vote standard and a resignation requirement for directors who fail to obtain a majority of votes cast, these bylaws generally preserve the board's discretion to reject the resignation letter and keep the director on the board indefinitely.

Consequential majority voting is also permitted under the MBCA. In states in which corporate law is based on the MBCA, mandatory departure of an unelected director can be tied to a fixed number of days following the election, unlike in Delaware where the departure must be tied to a resignation.

Is There Evidence That Shareholders Care about This Issue?

Yes. According to FactSet, the 89 *management* proposals from 2013–2016 for a majority vote standard received average support of 98 percent of shares voted (and 79 percent of shares

outstanding). In each year since 2007, average support for *shareholder* proposals requesting majority voting exceeded 50 percent. Since that year, average annual support has grown from 50.4 percent of votes cast "for" and "against" to 73 percent in 2016. Most of these shareholder proposals were opposed by management.

Would There Be Significant Director Turnover if Every Company Had to Replace Majority-Opposed Directors?

No. A tiny fraction of uncontested director elections result in failure to obtain majority support. In 2016, just 47 uncontested directors in the entire Russell 3000 did not receive majority support. These failures affected only 28 companies, or less than 1 percent of the index.

Is There Any Evidence That Having Majority Voting in Place Makes a Difference in Actual Director Turnover When Directors Fail to Obtain Majority Support?

Yes. Based on uncontested elections from 2013–2016 in which at least one director did not receive majority support, the vote requirement matters. Overall, a rejected uncontested director left the board 25 percent of the time. At "plurality plus" companies, the departure rate was nearly the same—24 percent, as of the close of 2016.

By contrast, at companies with majority voting, seven of nine directors who lost elections in the same period permanently left the board. The numbers involved are small but encouraging. Of course, any majority-opposed director at a company with consequential majority voting would have a 100 percent departure rate for unelected directors.

More details can be found on CII's Web site.[1] These findings are generally consistent with a 2012 study by the IRRC Institute and GMI Ratings, which found that "companies with majority standards are more likely than others to remove directors who receive minority support."[2]

Why Do So Few Companies Have Consequential Majority Voting?

Many boards view themselves as best qualified to make final decisions about the fate of majority-opposed directors, discounting shareholder views. Skeptics of consequential majority voting may argue that requiring an unelected director to leave the board could cause the company to be out of compliance with contracts, listing standards, or corporate governing documents. (In fact, consequential majority voting provides a grace period to maintain compliance.) Skeptics may also claim that consequential majority voting empowers "special interests." (This argument strikes CII as weak on its face, as holders of a majority of shares voting—the threshold for failure of a nominee under consequential majority vote standard—should not be considered a "special interest" in the context of a widely held public company with one-share, one-vote.)

Additionally, statutory and regulatory history bends toward plurality voting. Most states have corporate codes establishing plurality voting as the default standard, and companies are inclined to follow the default. Although some states have made majority voting the default, no state requires majority voting in uncontested director elections. CII petitioned the Delaware State Bar Association and the American Bar Association (ABA) to embrace majority voting, first as a default, then as a universal standard for publicly traded companies. The Delaware bar and the ABA declined to support the proposals. The major US stock exchanges do not require listed companies to elect directors by majority vote, despite CII requests to amend listing standards subject to SEC approval.[3]

Isn't the Threat of a Proxy Fight from Activist Shareholders Sufficient to Hold Boards Accountable to Shareholders, without Any Need for Shareholders to Have an Option to Vote against Directors in Routine, Uncontested Elections?

No. Even in uncontested situations, the election of directors should be more than an empty formality. Director elections are the basis for legitimacy of boards of directors in their exercise of power over property they do not own.

It is true that proxy fights for board seats are a critical accountability mechanism, but such fights entail substantial cost, are often disruptive, and in some cases can focus on financial engineering for the benefit of short-term shareholders. Directors should be accountable to all shareholders on a more routine basis. In addition to the traditional proxy fight, many companies now permit large long-term holders to use "proxy access" to nominate a small minority of directors.[4] However, we believe that voting rights should be meaningful without a requirement for a dissident nomination process and escalation to a proxy fight, even including a tool like proxy access that empowers only long-term shareholders. Moreover, proxy access has not been mandated market-wide.

Does the SEC Regulate How Companies Describe Their Voting Standards in SEC Filings?

Yes. While state law and companies' governing documents define the voting standard, the SEC regulates the contents of proxy statements and proxy cards.

But investors should be aware that some plurality-vote companies provide confusing descriptions of their vote standard in their SEC filings. In particular, some:

- Use terminology such as "majority voting" and "majority vote standard" in proxy statements, when in fact they are referring to the support threshold at which a director is required to submit a resignation letter for board consideration;

- Provide an "against" choice on the proxy card, potentially leading shareholders to believe such votes have an impact on the outcome of the election, when in fact they do not; and

- Avoid using the word "plurality" in the description of the vote requirement, for example by stating that majority voting applies unless certain external documents provide otherwise.

CII raised concerns in 2015 with the SEC about companies' use of confusing vote terminology.[5] The SEC on Oct. 26, 2016, proposed certain reforms.[6] The most beneficial of these, in CII's view, is the proposed requirement that plurality-vote companies disclose the effect of a "withhold" vote. This would make it crystal clear to investors that uncontested plurality elections guarantee victory for all nominees. However, the SEC proposal would not require the handful of plurality companies that provide an "against" choice to similarly disclose that voting "against" has no impact on the election's outcome. The SEC proposal would require companies with majority voting to provide "against" and "abstain" options, and bar them from providing a "withhold" choice.

Appendix 1: Sample Bylaw Language for Consequential Majority Voting

Sample Bylaw Language Compliant in Delaware[7]

If, as of the record date for a meeting of stockholders for which directors are to be elected, the number of nominees for election of directors equals the number of directors to be elected (an "Uncontested Election"), each director shall be elected by the vote of the majority of the votes cast with respect to that director's election at such meeting of stockholders, provided a quorum is present. For the purpose of an Uncontested Election, a majority of votes cast means that the number of votes "for" a director's election must exceed fifty percent (50%) of the votes cast with respect to that director's election. Votes "against" a director's election will count as votes cast, but "abstentions" and "broker non-votes" will not count as votes cast with respect to that director's election.

If, as of the record date for a meeting of stockholders for which directors are to be elected, the number of nominees for election of directors exceeds the number of directors to be elected, the nominees receiving a plurality of the votes cast by holders of shares entitled to vote in the election at a meeting at which a quorum is present shall be elected.

In order for any person to become a member of the Board of Directors, such person must agree to submit upon appointment or first election to the Board of Directors an irrevocable resignation, which resignation shall provide that it shall become effective, in the event of a stockholder vote in an Uncontested Election in which that person does not receive a majority of the votes cast with respect to that person's election as a director, at the earlier of (i) the selection of a replacement director by the Board of Directors, or (ii) 90 [or 180] days after certification of such stockholder vote. Acceptance by the Board of Directors is not a condition to the effectiveness of the irrevocable resignation.

Any director may resign at any time upon notice given in writing or by electronic transmission to the Chairman of the Board or to the Secretary. A resignation is effective when delivered unless the resignation specifies (i) a later effective date or (ii) an effective date determined upon the happening of an event or events (including but not limited to a failure to receive more than fifty percent (50%) of the votes cast in an election).

Sample Bylaw Language Compliant with the Model Business Corporation Act

Companies incorporated in states that generally follow the Model Business Corporation Act may consider the consequential majority voting bylaw at Microsoft,[8] which is incorporated in Washington, an MBCA state:

> 2.2 Election—Term of Office. At each annual shareholders' meeting the shareholders shall elect the directors to hold office until the next annual meeting of the shareholders and until their respective successors are elected and qualified. If the directors shall not have been elected at any annual meeting, they may be elected at a special meeting of shareholders called for that purpose in the manner provided by these Bylaws.
>
> Except as provided in Section 2.10 and in this paragraph, each director shall be elected by the vote of the majority of the votes cast. A majority of votes cast means that the number of shares cast "for" a director's election exceeds the number of votes cast "against" that director. The following shall not be votes cast: (a) a share whose ballot is marked as withheld; (b) a share otherwise present at the meeting but for which there is an abstention; and (c) a share otherwise present at the meeting for which a shareholder gives no authority or direction. In a contested election, the directors shall be elected by the vote of a plurality of the votes cast.

A contested election is one in which (a) on the last day for delivery of a notice under Section 1.13(a), a shareholder has complied with the requirements of Section 1.13 regarding one or more nominees, or on the last day for delivery of a notice under Section 1.14(g), an Eligible Shareholder has complied with the requirements of Section 1.14 regarding one or more nominees; and (b) prior to the date that notice of the meeting is given, the Board has not made a determination that none of the candidacies of the shareholder or Eligible Shareholder's nominees creates a bona fide election contest. For purposes of these Bylaws, it is assumed that on the last day for delivery of a notice under Section 1.13(a) or Section 1.14(g), there is a candidate nominated by the Board for each of the director positions to be voted on at the meeting. The following procedures apply in a non-contested election. A nominee who does not receive a majority vote shall not be elected. Except as otherwise provided in this paragraph, an incumbent director not elected because he or she does not receive a majority vote shall continue to serve as a holdover director until the earliest of (a) 90 days after the date on which an inspector determines the voting results as to that director pursuant to RCW 23B.07.290; (b) the date on which the Board appoints an individual to fill the office held by such director, which appointment shall constitute the filling of a vacancy by the Board pursuant to Section 2.10; or (c) the date of the director's resignation. Any vacancy resulting from the non-election of a director under this Section 2.2 may be filled by the Board as provided in Section 2.10. The Governance and Nominating Committee will consider promptly whether to fill the office of a nominee failing to receive a majority vote and make a recommendation to the Board about filling the office. The Board will act on the Governance and Nominating Committee's recommendation and within ninety (90) days after the certification of the shareholder vote will disclose publicly its decision. Except as provided in the next sentence, no director who failed to receive a majority vote for election will participate in the Governance and Nominating Committee recommendation or Board decision about filling his or her office. If no director receives a majority vote in an uncontested election, then the incumbent directors (a) will nominate a slate of directors and hold a special meeting for the purpose of electing those nominees as soon as practicable, and (b) may in the interim fill one or more offices with the same director(s) who will continue in office until their successors are elected.

Appendix 2: The Continuum of Regimes for Uncontested Director Elections

	Plurality Voting		**Majority Voting**	
	Strict Plurality (no resignation)	**Plurality Plus (rejectable resignation)**	**Majority Voting (rejectable resignation)**	**Consequential Majority Voting**
How do shareholders oppose[1] a nominee?	Withhold their vote	Withhold their vote	Vote against	Vote against
Who gets elected?	Nominees receiving the most "for" votes (*i.e.*, all nominees)	Nominees receiving the most "for" votes (*i.e.*, all nominees)	Nominees receiving more "for" votes than "against" votes	Nominees receiving more "for" votes than "against" votes
Must majority-opposed directors *immediately* depart from the board?	No. Majority-opposed directors are duly elected.	No. Majority-opposed directors are duly elected.	No. Unelected directors remain temporarily via holdover provision, though sometimes indefinitely.	No. Unelected directors remain only temporarily via holdover provision.

Must majority-opposed directors *eventually* depart from the board?	No	No. The "hard deadline" is the board's decision to accept or reject the resignation.	No. The "hard deadline" is the board's decision to accept or reject the resignation.	Yes. Unelected directors cannot serve beyond a grace period such as 90 or 180 days. (For Delaware companies, cutoff ties to irrevocable resignation; for MBCA companies, cutoff ties directly to calendar.)
Argument in favor	Assures board continuity	Enables board continuity while instituting a process for board to consider removal of majority-opposed directors	Same as Plurality Plus, but also denies majority-opposed directors the distinction of legally being re-elected	The only approach with "teeth." Places ultimate authority in the hands of the company's owners by removing the possibility of unelected directors indefinitely remaining on board
Argument against	No accountability to shareholders and no formal process for board to consider removing a majority-opposed director.	Legal election of all nominees remains certain. Resignation requirement provides discretion to reject the letter, which routinely happens.	Board retains discretion to keep unelected directors, and sometimes does so (albeit less often than at "plurality plus" companies.)	Does not accommodate scenario of unelected directors "curing" or pledging to resolve issue(s) perceived as having caused the defeat
Currently most prevalent among	Smaller-cap companies	Smaller-cap companies	Larger-cap companies	Not prevalent at present; early examples include Washington-incorporated Microsoft's MBCA-compliant version;[2] first Delaware company TBD
CII position	Opposes	Opposes	Accepts at companies with majority voting already in place and good-faith commitment to replace unelected directors within reasonable period	Supports as best practice

1 Shareholders who withhold their vote "oppose" a nominee only in unofficial capacity. Technically, every uncontested nominee in a plurality election receives 100 percent support and zero opposition because withholding a vote is the legal equivalent of an abstention.
2 *https://www.sec.gov/Archives/edgar/data/789019/000119312516641678/d219877dex32.htm*, last accessed Jan. 18, 2017.

Notes

1. *http://www.cii.org/majority_voting_directors*, last accessed Jan. 18, 2017.

2. IRRC Institute, *The Election of Corporate Directors: What Happens When Shareowners Withhold a Majority of Votes from Director Nominees?,* available at *https://irrcinstitute.org/wp-content/uploads/2015/09/Final-Election-of-Directors-GMI-Aug-20121.pdf,* last accessed Jan. 18, 2017.

3. Correspondence with the Delaware bar, the ABA and the exchanges can be found at *http://www.cii.org/majority_voting_directors*, last accessed Jan. 18, 2017.

4. *http://www.cii.org/proxy_access*, last accessed Jan. 18, 2017.

5. *http://www.cii.org/files/issues_and_advocacy/correspondence/2015/06-12-15%20CII%20Letter.pdf*, last accessed Jan. 18, 2017.

6. *https://www.sec.gov/rules/proposed/2016/34-79164.pdf*, p. 83, last accessed Jan. 18, 2017.

7. Following consultation with multiple Delaware securities law experts, CII believes this sample language complies with Delaware General Corporation Law as currently interpreted. There can be no accounting for future litigation in this area, however. Any company exploring revisions to its vote requirement should seek counsel on bylaw language, including counsel on how to address extraordinary circumstances such as multiple failed elections potentially triggering change-in-control provisions under material contracts and debt covenants.

8. Microsoft's complete bylaws, filed with the SEC in an 8-K on July 5, 2016, are available at *https://www.sec.gov/Archives/edgar/data/789019/000119312516641678/0001193125-16-641678-index.htm*, last accessed Jan. 18, 2017.

A New Role for the Annual Board Evaluation

By John Wilcox

Shareholders are scrutinizing the composition and activities of corporate boards more carefully than ever before. Board-centric annual meetings have become a showcase for director accountability and a referendum on the board's policies and performance. Board effectiveness and accountability have overtaken compliance as the quintessential corporate governance issue for shareholders voting their proxies at annual meetings. Director elections, even when uncontested, are no longer routine.

The era of technical governance reforms that lasted more than 30 years has largely run its course. External best practice standards are well established and no longer in dispute. With the exception of a few remaining skirmishes over issues such as shareholder access and dual class voting, there appear to be no new governance reform initiatives in the works. Instead, companies are facing a growing challenge in the form of shareholder activism that questions how effectively boards are implementing governance policies and how well companies are performing. Taking the lead from activists, shareholders and their advisors are scrutinizing board composition, director qualifications, the quality of the board's decisions, and their links to the company's strategic goals and long-term financial performance.

The shift to boardroom accountability should come as no surprise. It is the logical outcome of multiple factors that have shaped governance reforms and relations between companies and shareholders during recent years. These factors include:

- Shareholder activism in part triggered by the governance missteps of directors that focuses on financial performance, business strategy, and board accountability rather than just compliance with governance norms;
- Stewardship codes that require institutional investors to exercise greater diligence in monitoring portfolio companies and voting proxies in director elections;
- Growing awareness that environmental, societal, and governance (ESG) issues and other non-financial risk factors can have a significant impact on a company's sustainability and financial performance;
- The convergence of investor relations and corporate communications around board-level issues, in some cases reflecting an intentional blending of governance and branding strategies;
- Loosening constraints on communication between directors and shareholders in the wake of successful say-on-pay engagement campaigns;
- Dissatisfaction with the quality of disclosures by companies in voluntary "comply-or-explain" governance jurisdictions and demand for more informative and substantive narrative explanations; and
- The Integrated Reporting movement and accompanying efforts to introduce holistic management techniques and reporting under the oversight of the board of directors.

These developments have fueled an increase in activist campaigns that focus on business strategy and board effectiveness. The strategic questions asked by activists—and often by long-term shareholders following the activist lead—require answers from the directors as well as the management of targeted companies.

In an effort to increase transparency about board activities, companies have introduced a

 John Wilcox is Chair of Morrow Sodali.

variety of different types of communication. Detailed corporate governance policy statements, reports on ESG topics, and annual letters from boards explaining the way they are fulfilling the company's mission are increasingly common. Integrated summary annual reports are also being tested as a means to provide shareholders with business narratives that incorporate both board-level issues and financial results.

Current Board Evaluations

The annual board evaluation has even greater potential to shed light on boardroom activities.

Because board evaluation is virtually unregulated, companies have a great deal of flexibility with respect to both the process and its disclosure. The rules governing board evaluation are straightforward and non-prescriptive. New York Stock Exchange Section 303A.09 states: "The board should conduct a self-evaluation at least annually to determine whether it and its committees are functioning effectively." The UK's Corporate Governance Code goes further, requiring the annual report to explain "how performance evaluation of the board, its committees and its individual directors has been conducted" [Section B.6.1]. It also requires that "board evaluations of FTSE 350 companies should be externally facilitated at least every three years, and any other connections between external consultants and the company disclosed" [Section B.6.2]. Other important markets, such as Japan, have introduced board evaluation requirements with the objective of encouraging companies to meet global governance standards and thereby improve their productivity and economic performance.

Current board evaluations do not take advantage of the flexibility offered by minimal regulation. Instead, they focus on core legal and procedural matters: board committee structure, organizing documents, governance policies, numbers of meetings, attendance records, peer benchmarking, director independence, diversity, age, tenure, and contributions to the board skills matrix. They use detailed questionnaires for benchmarking and personal interviews to explore sensitive matters, such as the conduct of an individual director, the board's relations with the CEO and internal boardroom dynamics. The process resembles an annual physical exam in which doctor and patient participate in a private diagnostic review.

Reporting requirements for board evaluations have also been narrowly construed. Most companies go no further than disclosing in their proxy statement that the evaluation has been conducted. Details of the process, its findings, and any remedial actions taken by the board are generally not disclosed. Privacy and confidentiality take precedence.

There is extensive professional commentary in support of this limited concept of board self-assessment. Corporate governance practices must meet regulatory requirements, and boards need to understand how their policies compare with peer companies and best practice standards. Privacy and confidentiality are necessary to ensure that sensitive tasks such as the evaluation of an underperforming individual director will be undertaken rather than avoided.

However, there are also risks. A board evaluation that focuses exclusively on compliance and procedural matters may over time become a repetitive and formalistic box-ticking exercise. It may overlook issues that are important to external constituencies not present in the boardroom. Further, disclosure that contains no detail cannot answer shareholders' persistent questions about board qualifications and effectiveness.

A More Robust Evaluation Process Is Possible

A private diagnostic session does not have to be the exclusive model. The annual evaluation can be anything the board of directors and management want it to be. Because regulatory mandates give companies a virtual *carte blanche,* companies can exercise tight control

over both the process and its disclosure. They have discretion to design an evaluation that is appropriate for their particular circumstances, to decide what issues merit their attention, and to disclose as much or as little information as they believe is needed for an informative and convincing narrative.

They have flexibility to avoid the major concerns about greater board transparency:

- How to exceed regulatory limits on disclosure without incurring liability;
- How to safeguard confidential strategic information from competitors;
- How to avoid market confusion that may result from multiple voices speaking on behalf of the company; and
- How to maintain collegiality, privacy, and trust that are essential to effective board function.

Boards considering a more robust approach should ask several questions:

- Could the evaluation process make them better informed about the constituencies they represent?
- Could it help them understand how their conduct is viewed from perspectives outside the boardroom?
- When the risk of activism is rising—due to poor financial performance, a weak board, dissident shareholder resolutions, noncompliant governance, scandal, executive turnover, related-party transactions, or similar issues—could companies respond more effectively to these challenges or even avoid them by means of a more substantive board evaluation?
- Could a more comprehensive board evaluation process be an effective means for directors to improve perceptions, increase trust and minimize, if not avoid, confrontation and activism?

If the board answers these questions affirmatively, its plan for a comprehensive board evaluation should ask two additional questions:

- What constituencies are most affected by the board's current activities?
- What information does the board need in order to understand and respond to the expectations and concerns of these constituencies?

Shareholders and Other Constituents

The first and most important constituency for boards is the shareholders. They elect the directors, provide investment capital, and technically "own" the company. Shareholders are not a homogeneous group. They are constantly changing in response to multiple factors, both inside and outside the company, that influence their perceptions. The class of "institutional investors" predominates at most public companies, but they too are a highly diverse group pursuing a variety of financial goals: long-term, short-term, indexed, actively managed, international, domestic, private equity, pension funds (public, corporate, and private), mutual funds, hedge funds, strategic activists, high-speed traders, and other specialized investors and speculators. Retail shareholders, banks, brokers, intermediaries, and voting agents such as proxy advisory firms are important constituencies that are attentive to boardroom issues. Bondholders and potential future investors, critical to a company's ongoing capital structure and financial health, are audiences whose interests the board should understand.

Because every company has its own unique and constantly changing mix of owners and investors, the board should periodically be provided with surveillance reports covering ownership and market data. Management teams—corporate secretary, investor relations, marketing, customer relations, and research and development—gather this information throughout the year from a variety of sources and outside experts. Some of the most important data comes from the annual shareholders meeting.

Because the annual meeting is a board-centric event that centers on the election of directors, a wealth of data and insights can be culled from the meeting logistics, solicitation of proxies, vote tabulation, governance roadshows, shareholder communications, engagement campaigns, and other activities that peak around the annual meeting process. This information can tell boards not only who the company's shareholders are, but also what issues are of concern to them and how they perceive the company's management and board.

Annual meeting data can be supplemented with feedback from Investor Relations roadshows, securities analysts' reports, media and press coverage, market research, benchmarking, investor surveys, and peer and competitor analyses. These activities are routinely undertaken by management through the Investor Relations team, the corporate secretary, corporate communications and other departments. Their findings should be shared regularly with directors and reviewed in preparation for the annual board evaluation. With this information in hand, the directors will have a better understanding of why ownership changes have occurred, what they signify, whether owners understand the company's business strategy, how owners have responded to specific board initiatives, and whether company disclosures have adequately addressed owners' concerns.

In addition to shareholders and investors, the directors should be informed about any external constituencies that are affected either directly or indirectly by the board's activities and policies. Preparation for the board evaluation should take into account all aspects of the board's "job" and its core duties and responsibilities:

- Oversight of business strategy and long-term sustainability
- Capital structure and capital allocation
- Succession planning (both CEO and directors) and talent management
- Audit and accounting policy
- Executive and board compensation
- Risk oversight (including cybersecurity)
- Tone at the top, corporate culture, ethics, and reputation
- Policies on corporate governance, environmental practices, and responsible social behavior (ESG)

A comprehensive look at the full scope of these responsibilities may lead to unanticipated demands on the board. If the company faces a crisis, the board will have to assume a leading role. In such cases, the board must have the ability to quickly master unfamiliar issues and to understand the perspective of wide-ranging constituencies: communities serving and served by the company, governmental authorities, regulators, non-governmental organizations, special-interest advocacy groups, traditional media and social media, politicians, and international interests. There have been many recent examples of prominent companies facing banner-headline crises that have been unable to answer the key question: "Where was the board of directors?"

Reporting and Disclosure

Armed with an understanding of shareholder concerns and expectations, the board and management can exercise their judgment in deciding what and how much the board evaluation report should say. They have full discretion, within basic legal disclosure guidelines, to explain how their decisions have been reached and why they create value and serve business goals. For example, if disclosure about executive compensation in the company's proxy statement contains elements that do not comply with proxy advisors' standards, a board evaluation report could provide additional perspective on the policy and business considerations that influenced the board's decision. This disclosure might in turn reduce the need for an extensive engagement campaign. Experience has shown that shareholders will generally support noncompliant pay practices that have a valid business purpose.

The board evaluation report could be a vehicle to make the case for compensation and many other issues that rely on the board's business judgment.

The board evaluation report could also be particularly useful for companies to discuss ESG, non-financial risk factors, company culture, and other topics in which the board plays a central role. Although many companies publish mission statements and periodic reports on environmental practices, sustainability, health and safety, ethics, and business conduct, a discussion of these topics in a board evaluation report would have the potential to integrate board policies with strategic business decisions and financial goals. Indeed, this type of holistic presentation is a goal of the integrated reporting movement that is gaining support from leading companies around the world.

A potential downside is that comprehensive board evaluation reports could stimulate additional questions from shareholders and increase demand for discussion and engagement. Transparency can increase trust, but it can also invite dialogue. Regardless of this risk, boards should recognize the value of addressing and potentially resolving issues before they surface publicly in the form of shareholder resolutions, dissident campaigns, or an activist challenge. A well-informed board that understands the perspective and expectations of owners will be able to take the initiative, deal preemptively with problems, and avoid the risk of finding itself on the defensive in a public dispute. Conversely, shareholders who understand the board's thinking and business purpose will be less likely to seek engagement and more likely to cast their votes for the board at times when their support is most needed.

Conclusion

Thirty years of corporate governance reforms have concentrated attention on the critical role played by the directors of public companies. Shareholders recognize the board's importance but complain that they are asked to elect directors without being given sufficient information to make an informed decision. Today's board evaluations, mostly limited to compliance checks, peer comparisons, and examination of internal processes, are private affairs, with results that may be meaningful but are rarely visible to constituents outside the boardroom.

Annual board evaluations have the potential to do much more. A robust evaluation process can inform directors, give them a voice, and reassure a wide array of stakeholders that the board is representing their interests effectively. By providing early warning of constituents' concerns, the board evaluation process can also help the directors and management understand and deal with problems before they reach the stage of open confrontation.

Director Communications: Hacking Incidents & Cyber Threats

By John Evangelakos, Glen T. Schleyer, Marc Trevino, and Joshua B. Wright

The growth in cybersecurity threats combined with the increasing demands placed on outside directors create challenges that often go beyond the risks that public companies face from employee and client communications. If public companies cannot communicate quickly with directors or directors cannot easily share information and discuss options, corporate governance will suffer. On the other hand, outside directors often have professional responsibilities to multiple organizations and, accordingly, are more likely to rely on electronic communications that are outside of any particular company's technology resources.

Recent hacking incidents highlight the need for public companies to review their director communication practices to ensure that they are current and that they appropriately balance security and efficiency. In this regard, public companies may wish to consider exploring or re-exploring alternatives that fit with their information security framework, such as dedicated company email addresses or board portals. Each of these options has benefits, as well as some drawbacks, in terms of residual security, record-keeping, or efficiency. Regardless of the particular approach taken, public companies should periodically review their director communications practices in light of ongoing cybersecurity developments, regularly update directors on information security risks, company practices and response protocols in the event of compromise, and consider providing technology and security support for personal devices and home offices maintained by outside directors.

 John Evangelakos, Glen T. Schleyer and Marc Trevino are Partners, and Joshua B. Wright is an Associate, of Sullivan & Cromwell LLP.

Background

Corporations have various alternatives for electronic communications with directors. Many common means of communication, however, have been subject to highly publicized cyber incidents. Most recently, former Secretary of State Colin Powell and Democratic campaign strategist John Podesta became the victims of intrusions into their web-based email accounts through a deceptive email that requested login credentials.[1] These intrusions revealed politically and commercially sensitive information, including acquisition targets and strategies for Salesforce.com, where Secretary Powell was an outside director, and private email addresses of other outside directors. Although online board portals are generally accepted as more secure than web-based email accounts, several years ago a board portal reportedly was infiltrated by malicious code that allowed collection of confidential data stored on the platform. These incidents and the seemingly continuous advancements in computer hacking techniques emphasize that no technology should be considered immune from intrusion and that company practices relating to electronic communication with directors would benefit from periodic review and refreshment.

Potential Enhancements

As companies have continued to evaluate their practices, they have considered different systems for director communications, including the exclusive use of company email accounts by directors, and the adoption, or enhanced use, of online board portals. Each of these systems and policies has benefits and drawbacks, and each company will need to strike the right balance for itself and its directors. Additionally, companies have explored general IT policies such as

providing regular updates to directors on information security risks, company practices, and appropriate protocols in the event information is compromised, and providing technology and security support for personal devices and home offices maintained by outside directors.

Corporate Email Accounts for Directors

Assigning company email addresses to directors has the advantage of placing director communications under the same information security framework that applies to employee emails.

- Company protocols governing the strength and duration of passwords, the length of time that emails and attachments are retained, and filtering for unsafe content, are applied automatically.

- Enhanced security measures such as multifactor authentication, which requires two or more distinct forms of identification to access secure systems, also can be implemented.

- Policies and technologies can be updated without requiring special action on the part of directors. For instance, in the event a weakness is identified, a security patch or other measure can be implemented quickly without additional action by or further inconvenience to directors.

Some of the limitations often encountered with this approach include the following:

- A director may be less likely to see communications or notifications on a timely basis if they arrive via an account other than the director's primarily email. This concern could be addressed, in part, by non-confidential alerts sent to the director's primary email account when new materials have been sent to the company address. However, for directors that serve on multiple boards, the reduction in efficiency could be compounded if all of the companies required use of an internal email address for all company and board correspondence.

- Directors may have personal devices or computers that differ from those used by the company, which may limit effective and timely access to communications or lead to installation and troubleshooting issues (including with respect to security patches and printing), and could necessitate company access to the director's personal devices.

- A process that is not sufficiently streamlined could result in directors taking steps inconsistent with the policy, particularly in an emergency situation when timely review of materials is critical.

Board Portals for Director Communications

Many companies have adopted, or are exploring the use of, online board portals to facilitate director communications, either exclusively or in combination with other communication methods. Board portals are specialized web applications that disseminate board materials and communications through a web interface that may have several advantages.

- The organizational features of board portals can help to compensate for the inconvenience of requiring directors to manage a second set of login credentials. Rather than having board materials and communications contained in multiple emails, board portals present these resources in one place, in an organized format.

- The administrators of the board portal can exercise some control over how board materials and communications can be downloaded, viewed, and printed depending on, for example, the level of sensitivity of a particular document.

- Board portals can support customized document retention policies. Combined with their ability to organize related documents, this feature can promote efficient recordkeeping if used properly.

Some of the limitations often encountered with this approach include the following:

- Some board portals provide the option to capture metadata, including the extent and duration of directors' review of board materials. This information, while perhaps helpful in assessing the effectiveness of communications, has the potentially significant drawback that it could be attractive to plaintiffs in the event of litigation.

- Concerns have been expressed, including by some jurists, that electronic-only delivery of materials (as compared to delivery of paper copies) may hinder the ability of directors to adequately review, absorb, and provide feedback on the content of complex documents. To provide an adequate opportunity for thorough review, it may be advisable to permit directors to download and print, at least the most complex or important information from these files, or to provide for secure delivery of these materials in paper form.

- Board portals, in and of themselves, may not guarantee secure communications because they may present a high profile target for cyber intrusion and because they may be coupled with policies or devices that are less secure.

Training and Support

Cybersecurity threats have become a persistent concern for companies and, as the body responsible for oversight and as users of technology themselves, board members may benefit from periodic IT training and briefings regarding the company's communication systems, and from ongoing IT support in the use of those tools.

- If a company has an IT incident response plan, directors may benefit from a briefing on the plan, including how the directors' own technology usage fits into this plan. For example, directors can learn the signs of an attempted or successful intrusion and how to react to them.

- Directors could receive regular IT training for safe practices in the use of a company's communication systems. Such a program could be adapted from materials used for employees and management to highlight emerging cybersecurity threats and techniques, as well as protective strategies and considerations.

- As a supplement to their IT training, directors will likely benefit from ongoing IT support for their accounts and devices. Ideally, this would extend to their use of such technology outside of a formal corporate setting, such as providing support for a director's home office.

Observations and Implications

The information security landscape is evolving rapidly, and, while it seems clear that virtually all electronic communications systems are subject to intrusions, commercial, legal, and regulatory considerations dictate that companies should periodically review their director communications policies and procedures with an eye toward an appropriate balance among user convenience, administrative flexibility, and data security. This review should include the board, senior management, and IT personnel so that the applicable communication system and polices provide reasonable security while respecting the practical needs of directors. Directors and company employees would also benefit from periodic updates regarding the company's IT policies and recommended practices for information handling as well as developments in cybersecurity and cyber risk management.[2]

Notes

1. *See, e.g.*, Lorenzo Franceschi-Bicchierai, *How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts*, Motherboard/Vice Media (Oct. 20, 2016), available at *http://motherboard.vice.com/read/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts*, last accessed Jan. 17, 2017.

2. A summary of our firm's Cybersecurity Group and related resources is available at *https://sullcrom.com/cybersecurity,* last accessed Jan. 17, 2017. On December 1, 2016, Sullivan & Cromwell LLP hosted the 2016 Sullivan & Cromwell LLP / RANE Risk Management Summit to discuss pragmatic and proactive ways management and boards can mitigate enterprise cybersecurity risks.

Planning for Your Next Shareholder Meeting: Virtual-Only Meetings

By Lisa Fontenot and Linda Dang

In recent years, an increasing number of companies have opted to hold annual shareholder meetings exclusively online—that is, a virtual meeting without a corresponding physical meeting—rather than a virtual meeting in tandem with a physical meeting (the "hybrid" approach). While hybrid approaches are generally welcome or not opposed by investors and activist shareholders, some have criticized companies holding virtual-only annual meetings, asserting that virtual meetings limit the opportunity for shareholder participation in the meeting as well as engagement with management and the board. In spite of these criticisms, just as corporate use of the Internet and social media to communicate with stakeholders is growing, virtual meetings are on the rise.

In 2001, Inforte Corporation was the first company to hold a virtual-only meeting, following Delaware's 2000 amendment to its General Corporation Law permitting such meetings.[1] Though virtual meetings are still very much a minority of total annual shareholder meetings, more and more companies have been holding virtual meetings over the last few years: 27 virtual meetings in 2012, 35 in 2013, 53 in 2014 and 90 in 2015.[2] Broadridge Financial Solutions, an investor communications firm and a provider of a virtual meeting platform, reported 136 virtual meetings held in 2016 to date,[3] with particular popularity with recently publicly listed companies and technology companies. These include companies large and small, such as Intel, HP Inc., Hewlett Packard Enterprise, Fitbit, Yelp, NVIDIA, Sprint, Lululemon, Graco, GoPro, Rambus, El Pollo Loco, and Herman Miller.

 Lisa Fontenot is a partner, and Linda Dang is an associate, of Gibson, Dunn & Crutcher LLP.

Considerations for a Virtual Meeting

Benefits of Virtual Meetings

Virtual meetings present many potential advantages for companies and their shareholders. Advocates suggest that virtual meetings will increase shareholder participation as compared to physical-only meetings because of improved access. Shareholders who cannot attend in person due to location or other reasons can attend virtually and do not have to incur the time and costs of travel to a physical meeting. As an example, one company had only three shareholders attend its last physical meeting in 2008, while 186 shareholders attended its virtual meeting in 2009.[4] In addition, considering that thousands of annual shareholder meetings are held within a few weeks of each other, shareholders can participate in more virtual meetings than physical meetings.[5]

Similarly, companies may find virtual meetings appealing in their potential to reach as many shareholders as possible. Companies can also choose among different approaches to handling shareholder questions,[6] some of which allow companies to preview and prioritize important questions, eliminate duplicative items, and prepare more substantive or complete responses. Moreover, for some companies, the use of technology for the conduct of a shareholder meeting may be consistent with promoting the technology business of the company or enable a company to project a tech-savvy image.

A benefit to both shareholders and companies is the reduced cost of the annual meeting: A virtual meeting avoids the time, effort, and expense of organizing a physical meeting, including reserving a large venue and arranging for appropriate personnel and materials. With companies and investors becoming increasingly

global, virtual meetings can trim travel time and costs for shareholders, avoid traffic and other logistical delays, and be easier to schedule amid competing time demands. A virtual meeting may also be less disruptive to the company's daily routine, allowing management and other employees to return to their work more quickly. In the current atmosphere in which physical safety is always a concern, it is relatively easy to maintain security and control for a virtual meeting as compared to a live one. Lastly, holding the annual meeting virtually can reduce environmental impact, because there would be less travel and fewer printed materials regardless of the number of participants.

Challenges Presented by Virtual Meetings

Despite the potential advantages, some perceived challenges raised by virtual meetings cause certain institutional investors, such as the California Public Employees' Retirement System (CalPERS), the largest US public pension fund, and shareholder groups, such as the Council of Institutional Investors (CII), to oppose virtual meetings.[7] These investors assert that virtual meetings reduce the effectiveness of shareholder participation by eliminating shareholders' ability to meet with directors and express their concerns face-to-face. There is also concern that companies will manipulate shareholder questions to reduce any negative impact or redirect focus, by filtering, grouping, rephrasing, or even ignoring questions so that companies can manage questions and their responses to advance the company viewpoints. By selecting questions ahead of time, companies could choose not to answer hard questions that would be more difficult to avoid in person. In effect, virtual meetings could potentially allow companies to limit the influence of corporate governance activists.

Companies may fear that virtual meetings lack the personal connection with shareholders and communities that in-person meetings can convey. Virtual meetings may create more uncertainty in shareholder votes because shareholders can more easily attend virtual meetings than physical meetings and thus electronically vote or change votes at the last moment while attending a virtual meeting. Especially in contested elections, the certainty of proxies received in advance of physical meetings provides more comfort for companies about the projected outcome of votes. Shareholders who can attend a meeting virtually may be less inclined to vote by proxy in advance, making voting results less predictable and making it harder for companies to gauge whether their solicitation methods are effective or need to be adjusted. In proxy contests, parties could continue solicitation efforts via email up to the time of the virtual meeting, though a company's last-minute announcements or statements may similarly be more likely to affect votes. Some companies may avoid virtual meetings because of their reluctance to make their shareholder lists available online, as required by many states for virtual meetings. Moreover, without the personal touch present when face-to-face, virtual meetings may diminish companies' ability to resolve hostile or otherwise challenging questions as effectively as in physical meetings. Finally, to the extent that a virtual meeting broadcasts shareholder questions on a real-time basis, it could be more difficult for companies to manage disruptive participants than in a physical meeting.

Some prominent activist shareholders also oppose virtual meetings. For the 2017 proxy season, John Chevedden has submitted shareholder proposals to various companies requesting that the companies' board of directors adopt a governance policy to initiate or restore in-person annual meetings and publicize this policy to investors.[8] Chevedden has argued that in-person meetings serve an important function by enabling shareholders to better judge management's performance and plans.[9] Similarly, James McRitchie has written on his Web site about the negative impact of holding virtual annual meetings and advocated for shareholder proposals requiring physical meetings.[10]

Both CalPERS and CII believe that companies "should hold shareowner meetings by remote communication (so-called 'virtual' meetings) only as a supplement to traditional in-person shareowner meetings, not as a substitute" and

that "a virtual option, if used, should facilitate the opportunity for remote attendees to participate in the meeting to the same degree as in-person attendees."[11] California State Teachers' Retirement System (CalSTRS) has also expressed a preference for a hybrid meeting, though it acknowledged that "the technology is moving."[12] At this time, most other major institutional investors have not taken a public stance regarding virtual meetings.

Neither Institutional Shareholder Services (ISS) nor Glass Lewis have directly opposed virtual meetings in their guidelines, although ISS has indicated that it may make adverse recommendations when a company is using virtual-meeting technology to impede shareholder discussions or proposals.

Best practices for virtual meetings are continuing to evolve as more companies hold virtual meetings, so it may be difficult to predict investor response to specific practices.

Initial Considerations in Deciding Whether to Hold a Virtual Meeting

Governing Law and Documents

If a company desires to hold its meeting virtually, it first must confirm that the law of its state of incorporation permits virtual annual meetings and the requirements applicable to such meetings. Almost half of the states, including Delaware, permit virtual meetings.[13] However, some of these 22 states include conditions that, practically speaking, mean that virtual meetings likely would not be used: For example, California permits virtual meetings but only with the consent of each shareholder participating remotely.[14] Seventeen states and the District of Columbia do not permit virtual meetings but do permit hybrid meetings, and 11 states require a physical location for the shareholders' meeting while permitting remote participation.[15]

A Delaware corporation can hold its annual meeting virtually if it complies with certain statutory requirements. The company must "implement reasonable measures" to confirm that each person voting is a shareholder or proxyholder and to provide such persons with "a reasonable opportunity to participate in the meeting and to vote," including the ability to read or hear the meeting proceedings on a substantially concurrent basis.[16] The company must also maintain records of votes or other actions taken by the shareholder or proxyholder.[17]

After confirming that virtual meetings are allowed under the state law applicable to the company, the company should make note of any statutory conditions, such as disclosure or shareholder consent requirements or objection rights. For example, as noted previously, a company may also be required to make its shareholder list electronically available during the meeting.[18] A company must also confirm that its governing documents permit virtual meetings; for example, a company's bylaws often state where annual meetings are to be held and may need amendment to provide for virtual meetings. Notably, federal securities laws do not impose restrictions on how shareholder meetings are held. Similarly, while stock exchanges like the New York Stock Exchange and NASDAQ require listed companies to hold shareholder meetings, they also do not prohibit nor impose restrictions on virtual meetings.

Factors Influencing the Decision to Hold a Virtual Meeting

A company should assess typical shareholder attendance at its annual meeting and the interest in holding the annual meeting virtually of senior management and directors who may have concerns about investor reaction to a virtual meeting announcement or who may want the company to demonstrate its embrace of current technology. A company should also compare the costs and logistical efforts necessary for a physical meeting against those needed for a virtual meeting, which will include fees for the virtual meeting platform and may still include travel expenses for certain directors and management team members. Other factors include

whether any shareholder proposals are pending and the level of shareholder dissent, such as with respect to the company's performance or governance. The company should evaluate the risk of triggering shareholder activism if it announces an intent to hold its annual meeting virtually. There may be reasons why a physical meeting may be preferable, such as when director elections are contested or a significant business transaction or controversial proposal will be put to a shareholder vote. To date, no virtual meetings involving proxy contests have been held.

Planning for a Virtual Meeting

In 2012, a group of "interested constituencies, comprised of retail and institutional investors, public company representatives, as well as proxy and legal service providers" published guidelines for virtual meetings.[19] Chaired by a representative of CalSTRS and including members from the National Association of Corporate Directors, the Society for Corporate Governance (formerly known as the Society of Corporate Secretaries & Governance Professionals), AFL-CIO, NASDAQ, and others, this "Best Practices Working Group for Online Shareholder Participation in Annual Meetings" set forth the following principles for online shareholder participation in annual meetings:[20]

- Companies should "employ safeguards and mechanisms to protect [shareholder interests] and to ensure that companies are not using technology to avoid opportunities for dialogue that would otherwise be available at an in-person shareholder meeting."[21] Companies should adopt safeguards for shareholders' online participation by adopting policies and procedures that offer a similar level of transparency and interaction as a physical meeting. The policies and procedures should also address validation of attendees (to confirm that they are shareholders and proxyholders) and enable online voting.

- Companies should "maximize the use of technology" to make the meeting accessible to all shareholders. Steps to be considered include offering telephone or videoconferencing access "so that shareholders can call in to ask questions during the meeting," ensuring accessible technology "by utilizing a platform that accommodates most, if not all, shareholders," "providing a technical support line for shareholders," and "opening web lines and telephone lines in advance" for pre-meeting testing access.[22]

If a company decides to hold its annual meeting virtually, it may wish to proactively discuss the proposed change with key shareholders and explain the rationale for it. The company must also determine how it would handle shareholder questions, for example, whether all questions would be posted, and establishing what happens to questions received during the meeting that are not answered during the meeting.

A company has several options for hosting a virtual meeting (audio, video, telephone, or web), and a company's choice among those options will be guided by state legal requirements. Providers offer virtual meeting platforms on which companies can host their annual meetings and shareholders can attend and vote online. These commercial platforms can help companies comply with statutory requirements, such as Delaware's requirement to maintain records of votes and other shareholder actions. If possible, the company should leverage technology to allow attendees with different levels of technological savvy or resources to attend.

Conclusion

Though some originally thought that only small companies would use virtual meetings because larger, more well-known companies would want to use the annual meeting as a public relations opportunity and to avoid backlash from shareholder groups, large companies have now started holding virtual meetings. In deciding whether to hold a virtual meeting, companies should weigh the relative advantages and disadvantages applicable to their situations, which may include potential negative sentiment

from investors. With technological advances that enable the meetings to be more similar to physical meetings, the potential cost and time savings of virtual meetings may appeal to more companies.

Notes

1. *See* Eric Bomkamp, "Virtual-Only Shareholder Meetings: Inevitable Advance or Unwelcome Development?," *BNA's Corporate Counsel Weekly* (Feb. 23, 2011); *Virtual Shareholder Meetings*, TheCorporateCounsel.net, available at *http://www.thecorporatecounsel.net/member/LawFaqs/ElectronicStockholder.htm#a,* last accessed Jan. 17, 2017; subscription required.

2. *See* TheCorporateCounsel.net, *supra* n.1; Broadridge Financial Services, Inc., *2016 Proxy Season Key Statistics & Performance Rating* (based on shareholder meetings (*i.e.*, proxy "jobs") mailed between Mar. 1, 2016, and June 17, 2016), available at *http://media.broadridge.com/documents/Key-Statistics-and-Performance-Ratings-for-the-2016-Proxy-Season-new.pdf;* last accessed Jan. 17, 2017; Richard Daly, "Unless You're Warren Buffet, Your Next Shareholder Meeting Should be Online," *Forbes.com* (Apr. 28, 2016), available at *http://www.forbes.com/sites/richdaly/2016/04/28/unless-youre-warren-buffett-your-next-shareholder-meeting-should-be-online/#75ebdf7d42d2,* last accessed Jan. 17, 2017; Tom Braithwaite, "US companies embrace virtual annual meetings," *FT.com* (Mar. 11, 2016), available at *https://www.ft.com/content/874879c0-e664-11e5-bc31-138df2ae9ee6,* last accessed Jan. 17, 2017; subscription required.

3. *See* Broadridge, *supra* n.2.

4. *See* Daly, *supra* n.2.

5. *See id.*

6. For example, Broadridge offers companies three primary options for handling the question-and-answer segment of a virtual meeting: live questions submitted from shareholders via online text box, with only the company able to view incoming questions; telephone questions from shareholders during the meeting; or pre-meeting questions submitted by shareholders via a separate online portal. *See* TheCorporateCounsel.net, "Virtual Only Meetings: Nuts and Bolts" (Oct. 18, 2016), available at *https://www.thecorporatecounsel.net/Webcast/2016/10_18/,* last accessed Jan. 17, 2017.

7. *See* Braithwaite, *supra* n.2.

8. At least one shareholder proposal prohibiting virtual-only meetings was excluded under Rule 14a-8(i)(7) as relating to a company's ordinary business operations. *See EMC Corp.*, SEC Staff No-Action Letter (Mar. 7, 2002), available at *https://www.sec.gov/Archives/edgar/vprr/0202/02029901.pdf,* last accessed Jan. 17, 2017.

9. *See* Ross Kerber, "HP Moves Annual Meeting Online-Only as CEO Face Time Fades," Reuters (Feb. 12, 2015), available at *http://www.reuters.com/article/hp-meeting-internet-idUSL1N0VM1XM20150212,* last accessed Jan. 17, 2017.

10. *See* James McRitchie, "Virtual Meetings: Can Shareholder Proposals Stem the Tide?," *Corporate Governance* (May 11, 2016), available at *http://www.corpgov.net/2016/05/virtual-meetings-can-shareholder-proposals-stem-tide/,* last accessed Jan. 17, 2017.

11. *See* Council of Institutional Investors, Corporate Governance Policies 11 (updated Apr. 1, 2015), available at *http://www.cii.org/files/committees/policies/2015/04_01_15_corp_gov_policies.pdf,* last accessed Jan. 17, 2017; CalPERS, Global Governance Principals 63 (Mar. 16, 2015), available at *https://www.calpers.ca.gov/docs/forms-publications/global-principles-corporate-governance.pdf*, last accessed Jan. 17, 2017.

12. *See* Kerber, *supra* n.9.

13. *See* The Best Practices Working Group for Online Shareholder Participation in Annual Meetings, *Guidelines for Protecting and Enhancing Online Shareholder Participation in Annual Meetings* (June 2012), *http://www.calstrs.com/CorporateGovernance/shareholder_participation_annual_meetings.pdf,* last accessed Jan. 17, 2017; *see also* Del. Code. Ann. tit. 8, § 211.

14. *See* Best Practices Working Group, *supra* n.13; Cal. Corp. Code §§ 20(b), 600(a).

15. *See* Best Practices Working Group, *supra* n.13.

16. *See* Del. Code. Ann. tit. 8, § 211(a)(2).

17. *See id.*

18. *See* Best Practices Working Group, *supra* n.13.

19. *See id.*

20. *See id.*

21. *Id.*

22. *Id.*

Wolters Kluwer

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

TIMELY REPORT
Please Expedite

March/April 9900529061