CYBER SECURITY › SCOTT SINDER

Lots of Questions

What's the board's role in cyber security? Asking the right questions before, during and after a cyber event.

"Cyber security is no longer just an IT issue; it is an enterprise risk-management issue, and your board has to be involved."

You can find variants of this statement in almost any business-related cyber-security discussion (including some I have penned myself). The board oversight role also is embedded in every cyber-security protocol framework.

I am on several boards, and I advise several others. But I have been struggling with trying to determine what a good board should do to satisfy its responsibilities regarding cyber-security oversight. My Steptoe partners Jason Weinstein and Mike Vatis—whose expertise includes cyber-security compliance programs and incident response—authored the cyber incident scenario on page 42. It is interesting to me—and it seems wholly appropriate—that a board's role in its incident response scenario is simply to be informed.

Whether the board succeeds or fails in its oversight is probably best judged by how well prepared the organization is for the event and how it responds. At a very basic level, the board's ultimate success or failure can be judged by whether it asks the right questions.

In its recently issued report, *Connecting the dots: A proactive approach to cybersecurity oversight in the boardroom*, KPMG outlines a number of the concerns currently on board members' minds. Am I asking the right questions? Are we doing enough? These are just a couple. As that report and a plethora of others have noted, we definitely can do better.

The National Association of Corporate Directors has published a very instructive handbook, *Cyber-Risk Oversight*. It outlines five core cyber-security principles for directors and lists questions boards should be asking to satisfy these principles.

- **Principle 1:** Directors need to understand and approach cyber security as an enterprisewide risk management issue, not just an IT issue.
- **Principle 2:** Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
- **Principle 3:** Boards should have adequate access to cyber-security expertise, and discussions about cyber-risk management should be given regular and adequate time on the board's meeting agenda.
- **Principle 4:** Directors should expect management to establish an enterprisewide cyber-risk management framework with adequate staffing and budget.
- **Principle 5:** Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate or transfer through insurance, as well as specific plans associated with each approach.

The corporate directors group lists about two dozen core questions that boards should ask about their company's cyber-security regime. They really fall into three general buckets of questions:

1. What is the nature of our potential cyber threats? What are the cyber-security risks that confront the company? What are our most valuable assets that could be subject to these threats? How will we know if we have been attacked? Who are our likely adversaries? What testing have we done? What exposures do our business partners create for us?

2. What are we doing about it? What are the leading practices for cyber security, and where do our practices differ? Do our practices distinguish between general security and protection for our mission-critical assets? What vulnerabilities do we have for our mobile workforce? Is there any cyber-security related disagreement between management and our IT team? Do our business partners have cyber controls and policies in place? Are we monitoring their adherence to those controls and policies in any way? What do we do

REGULATORY NEWS TICKER

compensation. Payroll processors report each payroll to NYSIF with up-to-date figures for compensation and employee classification. Policies with annual premium between $1,000 and $250,000 or policies with annual premium greater than $2,000 for all contracting codes but roofing are eligible for PayGo when renewing workers comp insurance or obtaining new policy. » NYSIF adds QR code to its workers comp certificates to allow scanning for instant validation of certs and coverage via mobile devices. Red "no symbol" indicates invalid or voided cert. » Approves regulations for virtual currency Ether on Ethereum exchange, which will be operated by Gemini Trust Company. First state to authorize Ether. **www.dfs.ny.gov**

OHIO Names Sarah Morrison CEO and administrator of Bureau of Workers Compensation, succeeding Steve Buehrer, who left in April. Morrison has been in acting role since then and was BWC's chief legal officer before that.

» Department of Insurance granted permission to liquidate ACA co-op Coordinated Health Mutual, affecting InHealth Mutual policies. Policyholders must pay premiums, and providers must honor contracts for service during wind-down. **www.insurance.ohio.gov**

OKLAHOMA Insurance Commission officials warn they may require proposals for p-c rate hikes for earthquake coverage because of heavy market concentration and currently inadequate oversight on rates. Since 2011, 12 insurers have filed rate increases ranging from 4% to 300%. Total number of insurers writing earthquake has fallen from 140 in 2014 to 119 in 2016. Market share by top seven insurers in state is 66.5%. **www.oid.ok.gov**

OREGON Officials release online map and database spotlighting about 1,800 buildings in Portland susceptible to serious damage or collapse in earthquake. Mostly unreinforced masonry buildings built before the 1960s. Last time Portland

Send company news to **NewsEditor@LeadersEdgeMagazine.com**.

to evaluate the cyber regimes of potential acquisition targets during the M&A due diligence process? Do we have cyber insurance? Is it adequate? Do we participate in a group that shares information about identifying threats? What do we do with information we gain from that group? Do we have a robust training program? What else are we doing to raise firmwide cyber awareness? What do we do when we identify cyber-security deficiencies? Have we found any such deficiencies during the last year? What did we do about it?

3. What is our incident response plan if there is an attack? Do we have a plan? Under the plan, when will law enforcement and other relevant government entities be notified? What was our most significant cyber-security incident in the past quarter? What was our response? What constitutes a material cyber-security breach? What are we doing to stress test our plan?

In the unfortunate (but all too common) event that your company experiences a breach of cyber security, your leadership should be asking questions during and after the response that not only can help drive the immediate response but also may help to inform what adjustments should be made going forward. How did we learn of the breach? Did we discover it, or were we informed (or threatened) by an outside party? What was the impact of the breach? What have we done to contain the damage? What were the weaknesses in our system that allowed it to occur? What can we do to make sure this type of breach does not happen again?

At a very basic level, the board's ultimate success or failure can be judged by whether it asks the right questions.

Lots of questions, I know. I'm just glad that, when it comes to cyber-security issues, I get to ask more questions than I have to answer.

Sinder, The Council's chief legal officer, is a partner at Steptoe & Johnson.
ssinder@steptoe.com

EEOC Issues Final Wellness Rules

The U.S. Equal Employment Opportunity Commission issued in May final rules and guidance clarifying how the Americans with Disabilities Act and the Genetic Information Nondiscrimination Act affect employer-sponsored wellness programs. Despite recommendations from The Council and others to harmonize the EEOC's regulations with existing Affordable Care Act rules, there are notable discrepancies between the EEOC's and ACA's approaches to these employer programs.

In the preamble to the ADA rule, the EEOC addresses its recent litigation losses in the wellness program space, claiming those cases were "wrongly decided." The EEOC's final rule includes a provision stating that the ADA's safe harbors for health insurance, life insurance and other bona fide benefit plans—relied upon by courts that have ruled against the EEOC—do not apply to ADA-covered wellness programs. The EEOC's position likely will result in further legal challenges.

The ADA rule caps incentives for employees (reward or penalty, financial or in-kind) for all workplace wellness programs that include disability-related inquiries and/or medical examinations—including participatory programs and smoking cessation programs—at 30% of the cost of self-only coverage.

The GINA rule also includes a 30% cap but is far narrower in scope than the ACA or ADA rules. The GINA rule clarifies that employers may, under certain conditions, offer employees limited inducements for the employee's spouse to provide information about the spouse's manifestation of disease or disorder as part of a health risk assessment. The rule does not extend to information about employees' children nor to inducements for the provision of genetic information.

Both the ADA and GINA rules prohibit so-called "tiered health plans," which condition eligibility for particular health plans or benefit designs on participation in a wellness program.

The EEOC's rules are applicable on Jan. 1, 2017. For more information, see the Steptoe & Johnson summary at www.ciab.com/uploadedFiles/Advocacy/Secure/20160518_HighlightsfromEEOCfinalwellnessprogramrules.pdf.

did this, about 13% of identified structures were fully or partially upgraded; 8% were demolished. **http://insurance.oregon.gov/**

PENNSYLVANIA Department of Environmental Protection opens investigation into fracking's relationship to two small earthquakes near Hilcorp Energy operation in Mahoning Township in April. **http://www.insurance.pa.gov**

SOUTH DAKOTA Division of Insurance issues bulletin outlining changes to filing requirements for surplus lines policies now that Non-Admitted Insurance Multi-State Agreement is being dissolved. Last day to report new multistate policies to Surplus Lines Clearinghouse is Sept. 30, 2016. Policy endorsements or cancellations for policies effective on or before Sept. 30 may be reported to the clearinghouse until Sept. 30, 2017. Florida Surplus Lines Service Office will remain vendor for filings and premium tax submissions. As of Oct. 1, 2016, all new and renewal multistate surplus lines policies are to be filed as single-state policies with FSLSO when South Dakota is home state, and 100% of premium will be reported to and taxed by South Dakota. **http://dlr.sd.gov/insurance/**

VERMONT Department of Financial Regulation issues bulletin reminding carriers not to include non-cumulation provisions and endorsements in occurrence-based liability policies. Bulletin No. 189 says there has been an increase in such disallowed provisions in policy filings. Says insurers have not demonstrated actuarial relationship between pricing and non-cumulation clauses, provisions are inconsistent with nature of occurrence policies, and policyholders don't understand the technicalities of policy limit aggregation. **www.bishca.state.vt.us**