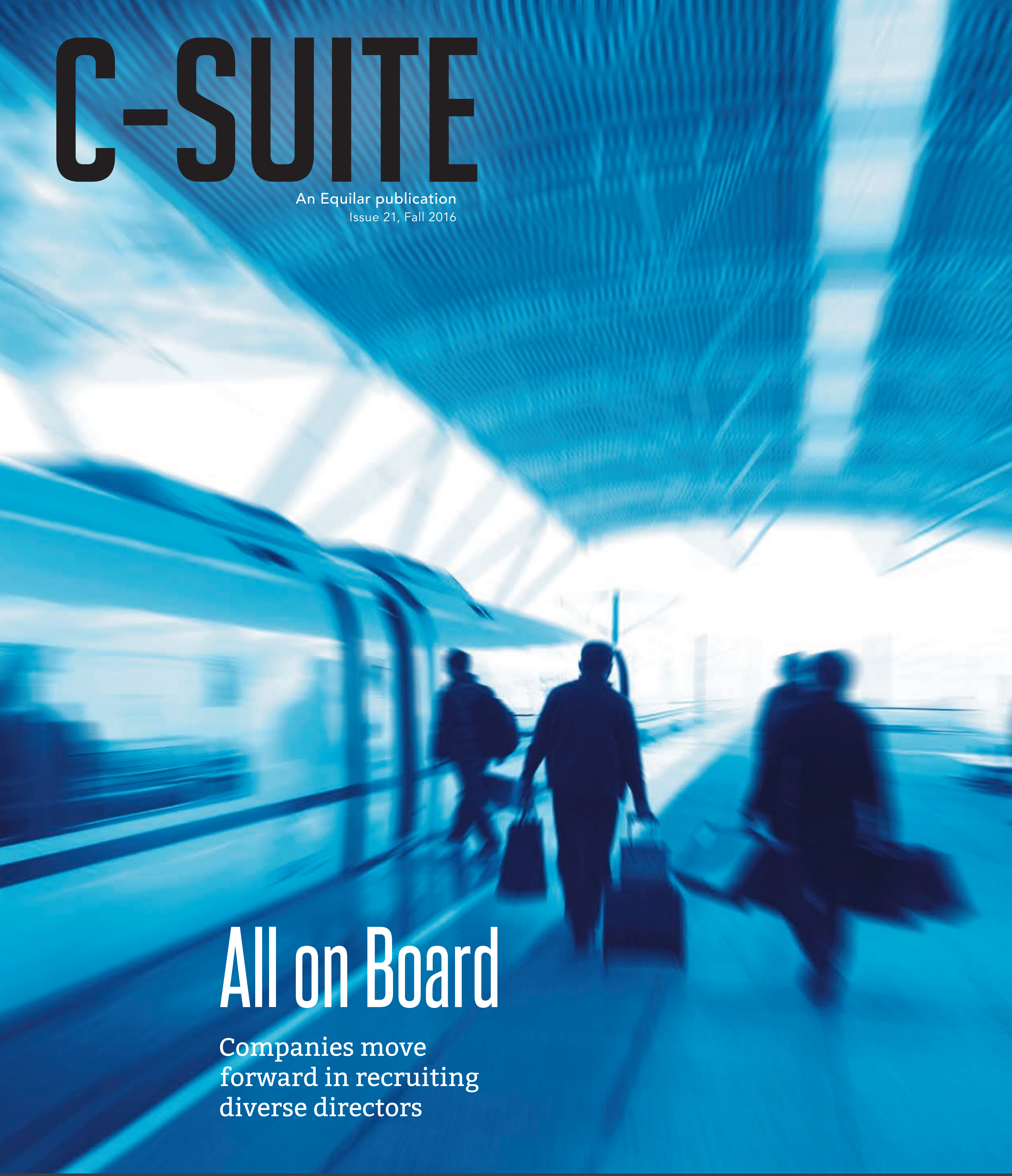

C-SUITE

An Equilar publication
Issue 21, Fall 2016

All on Board

Companies move forward in recruiting diverse directors

Narrowing the gap between investors and boards

Tips for joining your first board

Communicating the CEO pay ratio

Compensation trends around the world

Interviews with Cindie Jamison, Chair, Tractor Supply Co. and Keith Higgins, SEC

EQUILAR

Know Your Risk

Five key questions boards should be asking about cybersecurity

By Harriet Pearson

HOGAN LOVELLS

Effective board oversight of cybersecurity risk begins with asking the right questions. While the issue is complex, the board's mission is straightforward: To confirm that the essential elements of a risk management program are in place. This article describes what to probe in order to protect your organization and discharge your duties, presented by a seasoned lawyer and executive who has worked with boards, management and security professionals on these issues for two decades.

1. Do you know your risks?

As with any major challenge, the first step is to define the problem. Every company faces a different set of cybersecurity threats shaped by its position in the market, its geographic footprint and its reliance on technology. Boards should confirm that management has taken steps to understand the organization's posture in this respect and in the process educate themselves about the threats facing their company now and the threats on the horizon. Some cybersecurity threats are to data, like the well-known payment card breaches affecting retailers. Other threats are to access, like the distributed denial of service attacks on online sharing platform GitHub in 2015, which blocked consumers from the site for nearly six days. And still other threats might target a company's operations or reputation. What kinds of cyber actors target your sector? Are you susceptible to cause-related attacks? Which nation-states may take an interest

Key Questions

1. Has management identified known cybersecurity risks to the company?
2. Has management developed appropriate safeguards to protect systems and data?
3. Has management implemented methods to detect cybersecurity incidents?
4. Has management developed a process by which to handle a cybersecurity incident?
5. Has management developed a plan to recover and restore the company's operations that were impaired as a result of a cybersecurity incident?

in your activities? What are your biggest vulnerabilities and regulatory obligations, in terms of IT systems, data and people? And what about your third party vendors and relationships—what threats do their systems and activities face that could affect yours? If the board lacks an appropriately experienced member to take the lead on these and related inquiries, consider consulting with a specialist to assist.

Understanding your cybersecurity risk also requires understanding what you most want to protect. Confirm that management has taken steps to identify which data and systems are the company's "crown jewels" or mission-critical assets and has prioritized their defenses accordingly. There may be some kinds of data that require special care because of regulatory or contractual obligations, like personal health information or employee social security numbers. Other kinds of data, like key intellectual property assets, may be vital to the business plan. Knowing what most needs protecting, for both legal and broader business reasons, will help you confirm whether management is appropriately allocating limited cybersecurity resources.

*Harriet Pearson, a Partner at Hogan Lovells, is an internationally recognized corporate data privacy and cybersecurity pioneer. She can be reached at **harriet.pearson@hoganlovells.com**.*

2. Do you have and understand your organization's plan to addressing risk?

Once you know what is key to protect, the next set of questions aims to confirm that your organization has implemented appropriate safeguards. Starting with the Cybersecurity Framework issued by the National Institute for Standards and Technology and the ISO 27001 management standard, there are multiple industry-level standards for cybersecurity that can help identify a baseline of safeguards. How does your current program compare to those standards? Depending on the nature of the business, management may not need to implement every possible safeguard, but you will want to know why there are deviations from industry norms. A factor in investing in safeguards may be how much the company has transferred risk via cybersecurity insurance coverage. Consider whether the balance of insurance and investment is appropriate given your threat environment and legal obligations.

Implementing a cybersecurity program should look like implementing any other serious compliance program. Boards should be looking for a dedicated program, well-resourced and well-led, with the clear backing of management. There should be accountability mechanisms for the people responsible for the program and periodic assessments of their efforts. There should be trainings in place for the workforce on security and safe computing and established protocols for dealing with third parties, like law enforcement, in the event of an incident. It's also essential to understand how your company assesses the cybersecurity posture of its vendors and partners and what those third parties expect from you.

3. Do you know for sure if your organization can identify and detect problems?

The best-resourced cybersecurity program in the world is useless if there isn't a way to detect when something goes wrong. Boards and management should be fully briefed on how their program identifies a cybersecurity incident or potential threat and what triggers a response. Ask whether employees know to whom they should report if they get a phishing email or accidentally expose information. Ask the IT team how they detect whether a cybersecurity incident might turn into a breach. And make sure that your organization's cybersecurity program addresses the human factor: It's key to have a process in place to detect and address the threat of "insider" attacks that come from people, not programs.

4. Have you tested and practiced incident response?

When your organization detects a possible breach—now what? Every company should have a plan for what to do. Documented incident response plans should be in place and regularly practiced and updated—ideally annually or within the last 18 months. Ask what lessons the team learned from their last rehearsal or actual event and how those lessons have been incorporated into the current plan. Every company's needs are a little bit different, so boards and management will want to consider what makes a cybersecurity event material for their business. How will you know whether disclosure obligations are triggered? Are appropriately experienced legal counsel looped in early? And when will senior management and the board be involved? Companies that make a plan for trouble when things are calm will be better able to respond rapidly when something goes wrong.

5. And most importantly, have you prepared for the inevitable?

In this day and age, the question isn't if your company will have a cybersecurity incident. It's when. Effective cybersecurity risk management doesn't just mean preparing for how to respond. It also means preparing for how to cope. Make sure your company has backup plans if cybersecurity incidents impair operations. Is there a business continuity or recovery plan? Are your core systems backed up? What does recovering from the back up require? And just like with response, practicing how to deal with a loss of operations is key. Check with your cybersecurity team to ensure they are testing their plan to recover and restore operations at least every 18 months and incorporating lessons learned.

An effective cybersecurity program is one that identifies the risks, adopts the approach best-suited for the organization, detects problems, plans for incidents and prepares for the worst. Boards that keep these five core considerations in mind will be in the position to confirm that their companies are appropriately managing the security risks of an interconnected world. CS

EQUILAR
Data. Decisions. Results.

Data.

Equilar is the #1 provider of executive data, collecting information on more than 140,000 executives and board members from thousands of public companies.

Decisions.

Our cloud-based platforms organize executive data into easily digestible formats, delivering compensation benchmarking, board assessment and shareholder engagement tools with accuracy and integrity to inform better business decisions.

Results.

Our engagement tools bring together companies, shareholders, and third-party advisors and service providers to drive exceptional results.

Find out why institutional investors with more than $13 trillion in assets, more than 60% of the Fortune 500, and the world's top media outlets such as *The New York Times, Bloomberg, Forbes, Associated Press, CNN Money, CNBC* and *The Wall Street Journal* trust Equilar.

Learn more at: www.equilar.com

Equilar TrueView
Benchmark with the best.

Equilar Market Peers
No art. Just science.

Equilar Pay for Performance
Win your Say on Pay vote.

Equilar BoardEdge
Build a high-performing board.

Education Forums
Learn from the experts.

Knowledge Center
Stay updated on today's governance topics.

Custom Research
Custom data. On demand.