


Corporate Boards' Oversight Of Cyber Risks Is Too Passive



Harry G. Broadman, CONTRIBUTOR

I advise, speak, testify and write on global markets, business strategy, risk and governance. [FULL BIO](#)

Opinions expressed by Forbes Contributors are their own. 

EDITOR'S PICK

November 28, 2018 @ 04:04 PM



Many corporate boards have made significant progress about understanding the importance of cyber security to the competitive health and sustainability of the companies they oversee. They've certainly gotten the message that cyber security is not just an IT issue. And, within the portion of board meetings devoted to risk assessment, cyber security is almost always one of the top items on the agenda.

But most board directors have yet to move far enough along to become as effectively equipped as they should be to intelligently gauge the extent to which their firms' management teams are at the top of their games in the war on corporate cyber-attacks. Few board members engage C-suite executives in meaningful dialogue on the *specific* strategies they're undertaking to reduce vulnerabilities to hacks and why *particular approaches rather than others* are being employed.

I know this firsthand: both from the corporate boards on which I serve and from the boards I advise on business growth and risk-mitigation strategy, especially boards of companies where international transactions are important to their lifeblood—hardly a unique characteristic of many firms in today's global economic ecosystem in which *all* of us make decisions one way or another.

The bald fact is that many board members are intimidated to ask the members of their C-suite executive teams who are most centrally responsible for cyber security—usually chief information security officers (CISOs)—all but the most general technical questions. And even then, the issues that board directors raise with the C-suite almost always focus on the magnitude of the *problem* and the degree to which the CISOs believe they have *existing* threats contained.

And, for the CISOs, they tend to have an incentive to give briefings to their boards about cyber security in relatively dumbed-down language. It's been my experience that it is a rare CISO that discusses with his or her board the nitty gritty of the actual *solutions* their teams have either already rolled out or are contemplating doing so.

Most members of a corporate board become well-versed to ask their firms' Chief Financial Officers (CFOs) technical questions about financial reporting and related details. Yet when it comes to cyber, intimidation seems to kick in. It doesn't have to be this way. And, it shouldn't.

It's actually not a herculean feat for board directors to become sufficiently facile in understanding the types of solutions available to reduce cyber risks to which intra-enterprise communications have been exposed or to prevent them from being so.

Indeed, boards should be able to equip themselves with the knowledge necessary to have meaningful exchanges with CISOs to discuss the practical pros and cons of various remedies, including how various options can affect internal governance, employee productivity, and document retention among other dimensions.

The real irony in all of this is that it's often the communications within the boardroom and within the C-suite *themselves* where the most sensitive corporate issues are being discussed. These are where the payoff for cyber penetration is highest. It's therefore no surprise these are the prime targets for hackers.

They are the highest value targets for two reasons.

The most obvious is these locales are at the pinnacle of a business' decision-making apparatus and thus where the most closely held commercial information is expected to be internally communicated.

In the boardroom, such communications can range from details of negotiations over the share value of a bid made for the acquisition of the company (or a bid made by the company for an acquisition target) to polling among board members about the degree to which there remains confidence for retaining (or firing) the company's CEO who has been accused of engaging in an egregious business practice.

Within the C-suite, they might pertain to topics such as an in-house assessment of the bottom line impacts of the company's proposed new pricing strategy vis a vis its competitors or information on the extent to which a dangerous safety defect has just been discovered internally in the manufacturing process of the firm's best-selling product.

The second reason is even more pernicious: these are where the internal communications take place about the specific methods the firm is employing to fix the hardware and/or software vulnerabilities that exposed high valued communications in the first place. If the hackers are able to determine the exact solutions being applied by say, the chief information security officer, not only does vulnerability remain, but the firm has now unwillingly provided information about its internal decision-making process on how it is handling cyber security. This is the grand prize for hackers.

In light of this, one might ask what is the general tenor of the conversations underway and the actions undertaken about cyber security in corporate boardrooms today, especially interchanges between directors and members of C-suites?

While loads of surveys have been taken to get at the answer to such a question—indeed rarely does a month go by when there isn't a number of corporate board-related publications reporting on such surveys—few surveys, if any, have been large enough to systematically capture a *representative cross-sectoral* sample to provide meaningful results.

Worse still, the survey instruments generally utilized pose *perception-based* questions rather than incorporating a *data-driven, fact-based methodology* that is, one that quantifies empirically the actual number of times specific actions have or have not actually taken by board members.

From my own and others' observations—to be sure an admittedly a small and not purported to be a representative sample and thus not necessarily true for all corporate boards—the “typical” conversation on cyber at the board level tends to focus on the following types of broad questions posed by directors to CISOs:

- Are we secure?
- How do we know if we've been breached?
- How does our security program compare with industry peers?
- Do we have enough resources for our cybersecurity program?
- How effective is our security program, and is our investment properly aligned?

These are certainly important questions to be asked (and answered). But they should be seen only as conversation starters. Why? Because in and of themselves, they do not provide the basis for board directors to make well-informed judgments about *comparative* solutions for intra-enterprise communications systems to reduce vulnerability to cyber-attacks.

I emphasize “comparative” because there is an array of communications solutions and most involve tradeoffs of one type or another. And such solutions need to incorporate both cyber-secure email *and* [messaging](#), the latter being particularly important as Millennials climb the corporate ranks. They have grown up in a messaging-only world and that is the way they will continue to communicate even in the workplace whether one likes it or not.

There is an emerging consensus that an ideal solution would likely be one that:

- throughout the company—from the “factory floor” to the boardroom—a firm’s email and messaging communications, telephone conversations, videos and files would be subject to bona fide end-to-end encryption, employing state of the art protocols (both those currently available with provisions for continuous updating)
- there is an inviting, productive user experience,
- agile document permission and retention controls exist, and
- sound yet flexible internal governance practices can be easily employed (for example, the ability to segregate access to certain communications within the firm, so as to avoid the risk of the “in plain view doctrine”, among other risks).

Against this backdrop, here then are some of the most fruitful types of questions board directors and C-suite executives, especially the CISO and his/her team, should be directly discussing about communication system solutions to enhance a company’s cyber-security:

- Do both the email and messaging systems used by *all* the firm’s employees, including the C-suite and the board of directors, embody best-in-class *end-to-end encryption*?
- Is there any way that the company’s internet service providers (ISPs) are able to *decrypt* the company’s communications on *their* servers?
- What is the process by which the company *regularly benchmarks* the communications software being used compared with alternatives coming on the market?
- How automatic and complex is the system’s security update process?
- Is the system currently in place an app and cloud-based solution, or does it require *expensive infrastructure or proprietary hardware*?
- Does the system *work across* all operating systems and with all mobile devices, tablets, and desktops?
- Is the system fully deployable *globally*? What steps are utilized to reduce exposure to hacks for the company’s employees working in the *world’s most cyber risky markets*?
- Does the C-suite routinely deploy firm-wide surveys to assess the extent to which there are employees who don’t find the current system’s *user experience friendly*? How *widespread* is any negative feedback? What are the specific steps employed to address it?
- How agile is the system’s ability to *compartmentalize* internal communications and documents?
- How robust is the firm’s communications software in terms of providing for systematic enterprise-wide information *life cycle controls*, including both destruction and retention of high-risk or proprietary internal documents and data?

Harry G. Broadman is a Partner and Chair of the Emerging Markets Practice at the Berkeley Research Group LLC, a global consulting firm, where he works on international trade and investment disputes; antitrust and regulatory litigation; market intelligence and investigations related to reputational and corruption risks; and corporate strategy and operations. He is also a member of the Johns Hopkins University Faculty, a Board Governance Fellow and Master Workshop Faculty Member at the National Association of Corporate Directors (NACD) and serves as an independent director on several corporate boards. He is former United States Assistant Trade Representative; Senior Managing Director at PricewaterhouseCoopers and PwC Chief Economist; Managing Director at Albright Capital Management; a World Bank official in China, Russia The Balkans and Africa; Chief of Staff of the President’s Council of Economic Advisers; a faculty member at Harvard University; on the RAND Corporation staff; and a fellow at the Brookings Institution.

Contact: <http://www.harrygbroadman.com>

The link to this column is: <http://www.forbes.com/sites/harrybroadman>