GULF NEWS
ANALYSIS
Published: April 4, 2019

Corporate Boards Need Courage for Cyber Threat Solutions

These risks aren't more technical than financial issues they confront

By Harry G. Broadman, Special to Gulf News

At first glance, Corporate boards across the globe have made significant progress about understanding the importance of cyber security to the competitive health and sustainability of the companies they oversee. They've gotten the message that cyber security is not just an IT issue. In 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 the management teams they supervise 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 truth 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. As a result, 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. Sadly, boards rarely deal with solutions to strengthen cyber-security.

Compounding this is that CISOs 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 details of potential remedies their teams have either already rolled out or are contemplating doing so.

In contrast, most members of a corporate board become well-versed to ask their firms' Chief Financial Officers (CFOs) very technical questions about financial reporting and related details. But when it comes to cyber, boards shy away from getting in to the details. It doesn't have to be this way. Indeed, it shouldn't.

It's my experience that it is not a huge 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. Directors can 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 irony 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. After all they 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. They are the grand prizes for hackers.

So, 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?

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: (i) Are we secure? (ii) How do we know if we've been breached? (iii) How does our security program compare with industry peers? (iv) Do we have enough resources for our cybersecurity program? And, (iv) 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. 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 outline in detail the more relevant questions board directors should ask their management teams here at the end of a longer *Forbes* column from which the current column draws.)

It's high time for corporate boards of directors to expand their knowledge about what it takes to make the firms they oversee cyber secure. But first, they have to find the courage to want to do so.

Harry G. Broadman is Managing Director and Practice Chair at the Berkeley Research Group LLC, a global consulting firm focused on international trade, investment, antitrust and regulatory litigation and disputes, arbitration and investigations; corporate finance; and business strategy and operations. He is a member of the Johns Hopkins Faculty 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; 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 https://gulfnews.com/business/analysis/corporate-boards-need-courage-for-cyber-threat-solutions-1.63050443