Connecting Cybersecurity to Your Business Strategy

Boards Must Take a Stronger Role, and Ask New Questions, In Leading Battle to Protect Data

As cyber attacks and data breaches continue to make headlines and shake whole industries, a whopping 87 percent of board directors and C-level execs say they lack confidence in their organization's level of cybersecurity.[1] As such concerns mount, it's become clear that organizations have been looking at cybersecurity through the wrong lens.

Traditionally, cybersecurity teams have focused on whether their individual controls functioned adequately, if countermeasures were appropriately implemented and if coverage was sufficient to close risk gaps. This functional approach to cybersecurity is inadequate to deal with the ever-growing complexity of modern IT environments.

Today, an effective cybersecurity program must be tied to the company's business strategy. Companies need to determine what specific controls and countermeasures offset the most risk based on the specific risks that might arise given their mission, operating environment and the type of attacks they're likely to encounter.

Make a Commitment

As with any element of business strategy, the board must take a key role in cybersecurity.

The board can demonstrate commitment by establishing a role to lead this effort such as a CISO or CSO and provide the budget to accomplish the task. It's equally critical for everyone to be on the same page, which is often not the case today. In a recent survey, 90 percent of board members said the primary benefits of cybersecurity were "data protection" followed by "brand protection." However, CISOs listed those two at the bottom of their lists — in their view, cybersecurity's highest value was in "security guidance" and "business enabler."[2]

This disconnect shows that boards are not clearly establishing what the business needs are from a cybersecurity program because they have not tied security to strategic objectives.

Board members need a clear understanding of how proposed investments in cybersecurity are directed to the most significant cybersecurity risks. They can also ensure that security risks are integrated into the overall enterprise risk analysis as well as make those risks part of any M&A discussions.

Ask Three Questions

When considering how cybersecurity ties into business strategy, board members should consider three questions:

Does your organization have a comprehensive list of cyber risks that is informed by your strategic objectives? The cybersecurity needs of each company are as unique as a set of fingerprints. Business strategies hinge on new technology, like IoT, that offer both new levels of reward and new levels of risk that must be balanced and addressed.

Are you relying solely on regulatory frameworks or industry specific standards? These often lag the current threat landscape and don't build the organization's resilience. Compliance-driven efforts, though ensuring a minimum baseline is achieved, do not account for the organization's unique risks.

Are you putting too much trust in third-party providers? While strong relationships can provide reassurance, the lack of transparency often limits their impact of institutionalizing knowledge and building in-house capabilities.

Keep Informed Using New Tools

To lead an effective cybersecurity effort, board members need the best and most current information they can gather to inform their decisions. However, the National Association of Corporate Directors (NACD) recently released a survey of more than 600 corporate board directors and professionals that found only 19 percent believe their boards have a high-level of understanding of cybersecurity risks.[3]

Fortunately, there are new tools that can arm the boards with greater knowledge. For example, the CMMI Cybermaturity Platform, debuting in April, is designed to build board confidence by aligning strategic objectives with pragmatic insights of security risks. The dynamic architecture updates are based upon the changing landscape to provide current and relevant security best practices. The information is presented in graphical constructs that are familiar to boards and in terms that inform boards to make better decisions.

The ability to achieve business goals and objectives is tied to effectively managing cybersecurity risk. Boards must take an aggressive role in ensuring the connection of cybersecurity to business strategy is just as strong as the business strategy itself.

Cybermaturity.cmmiinstitute.com

Sources:

1. https://www.directorsandboards.com/news/directors-lack-cybersecurity-confidence
2. https://www.risklens.com/blog/cisos-and-boards-of-directors-are-far-apart-but-can-close-the-gap-new-survey-says
3. https://www.nacdonline.org/AboutUs/NACDInTheNews.cfm?ItemNumber=38735