BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

"According to the Gartner 2020 Board of Directors Survey, cybersecurity-related risk is rated as the second-highest source of risk for the enterprise, following regulatory compliance risk. . . . CISOs must expect executive conversations to shift away from performance and health-related discussions to risk-oriented and value-driven exercises." (Gartner Inc., January 28, 2021)

November 15, 2021

Bridging the Gap – Enabling More Constructive Cybersecurity Discussions Between Boards and CISOs

By Kevin P. Gowen

There is a critical need to bridge the cyber risk mitigation language barrier between boards and Chief Information Security Officers (CISOs). Today more than ever boards are focused on their cyber risk oversight obligations, yet few board members are cybersecurity experts. CISOs typically speak the language of cyber risks through a sometimes highly technical lens. This nomenclature gap creates ongoing organizational risks as board members seek additional insights to better inform their oversight responsibilities. Language friction causes some CISOs to miss an important opportunity to effectively outline the business impact of proposed mitigation investments and gain critical buy-in for their efforts. The good news: acknowledging the gap and working together to address it, boards and CISOs can align the language of cyber risk and, most importantly, understand organizational efforts to mitigate that often headline making risk.

Cyber risk language issues are coming at a time when the structure of many businesses is changing rapidly. Today we live in the age of the "extended enterprise" with increasingly complex outsourcing and supply chains that inevitably increase cyber risks. While the best approaches to board cyber risk oversight will depend on the company and industry, the starting point must always be an accurate understanding of the specific cybersecurity risks that are relevant to an organization. Without that understanding it's difficult for boards to fulfill their critically important oversight role.

LOOKING OUTSIDE – PARTNERING WITH YOUR CISO TO BETTER UNDERSTAND TODAY'S INTIMIDATING CYBER THREAT LANDSCAPE

Helping boards understand how the organizations they oversee monitor, assess and address the evolving cyber risk landscape is a fundamental CISO responsibility. CISO's typically:

- Provide the board with an accurate understanding of the evolving cyber landscape in the context of the organization's business and risk appetite framework.
- Discuss how organizational cybersecurity programs effectively mitigate risk.
- Put the day's cybersecurity headlines into context.
- Inform the board about new approaches to better understanding cyber risks (for example, using continuous monitoring to understand inherent cyber risk further down complex outsourcing chains).
- Take the board through tabletop exercises that simulate an actual cybersecurity attack on the organization they oversee.
- Make the board comfortable with the forensic processes already in place to be utilized in the event of a successful cyber-attack.
- Help the board understand incremental resources and programs that might be required as the threat landscape changes and as tools to meet new threats come online.

One of the keys to board understanding of the potential impact of emerging cyber risks is to - wherever possible - quantify those risks in financial terms that boards can interpret. One commonly used approach is the FAIR (Factor Analysis of Information Risk) model developed by the FAIR Institute. The approach is valuable in many situations because it can translate an organization's cyber risk and loss exposure into monetary terms. Models such as FAIR are at their best in quantifying sharply defined elements of the company's risk but become less relevant when multiple elements and types of risks are considered together. Most financial models have a more difficult time when considering cascading risks, the impact that comes when one risk triggers another and the impact of multiple risks exceeds the sum of individual risks and creates compounded results. Anticipating and quantifying the impact of cascading risks remains a significant challenge.

Cyber risk is evaluated without any offsetting controls (inherent risk) and again when a full suite of controls is applied to mitigate risks (residual risks). All risk management organizations evaluate and rank order cyber exposures without any controls applied because that measure serves as a "worst case" indicator of financial impact to an organization in the event of a successful attack. The inherent risk of a threat type can vary, and boards should be satisfied that an organization has a structured approach toward understanding the impact and the likelihood of given risks. Regulatory and compliance requirements, the volume and type of confidential data the organization holds, the potential reputational impact of cyber events, and the level of security training and awareness of the workforce are among the considerations in identifying inherent risk.

CISOs should educate the board about how they determine which risks and threats are most relevant to the organization. It's important for the board to understand which risks pose less of an organizational threat and those that are critically important. When there is a risk or technology board committee in place to provide oversight of cybersecurity, management should provide regular updates on the risk profile and specific approaches toward mitigation of the most significant risks, and to convey the continued alignment of the security program with current risks and threats.

Questions Boards Should Consider:

- Does the board have an accurate sense of the cyber risk and threat landscape and the greatest threats to the enterprise?
- Does the board understand the company's inherent cyber risk profile and how that profile aligns with the firm's risk appetite?
- Does the board understand and approve of how the company maintains threat awareness and intelligence?
- Does the company participate in government and industry cyber risk information sharing organizations?
- Are external services utilized to provide threat intelligence?

LOOKING INSIDE – UNDERSTANDING AND AFFIRMING YOUR FIRM'S SECURITY POSTURE

An organization's security posture reflects the strength of its security policies and controls and how effectively they mitigate risk. Security posture is dynamic and reflects both the changing threat landscape and an organization's ability to make continued progress in strengthening its cybersecurity program.

Seasoned boards understand that the ability of any cybersecurity program to successfully drive down inherent risk while maintaining alignment with risk appetite is a strong indicator of a program's return on investment. Boards should be comfortable that the CISO has identified the business' most critical assets, has an effective plan for their protection, and is executing against that plan.

CISO'S should review the effectiveness of their organization's cybersecurity controls regularly and report results to the board. A common approach to gauge effectiveness relies on a subjective "strength of controls," a technique often used in Risk-Control Self Assessments. Strength of controls reflects the effectiveness of the security systems to identify and respond to malicious activity. In part because of the inherent subjectivity of the strength of controls approach, it deserves board level questioning and challenge. How are subjective judgements being made and how, if at all, are they being validated?

Third-party challenges such as penetration testing are an important way to develop an independent perspective on an organization's security posture and boards should clearly understand their role. Most internal security teams are only familiar with what they see inside organizational walls, but experienced third-parties, or internal "red teams" with independent challenge as a focused mission, bring a broader perspective to the assessment that is informed by a far wider range of experiences. CISOs should have a robust program for incorporating third-party security reviews, at both the tactical and the strategic levels. Results of those reviews, which provide guidance on areas of strengths and of opportunity, help form the security organization's strategic plan.

The ability to attract, develop, and retain cybersecurity talent is a critical issue for security leaders and boards. Management should have and share its process for understanding current cyber talent to help prioritize training and hiring activities. Input from evaluating the changing threat landscape, an assessment of the program's effectiveness and input from independent testing and reviews inform current and projected talent requirements.

Questions Boards Should Consider:

- Has the enterprise assessed its ability to detect and protect against the most critical threats?
- How does the cyber program incorporate organization-wide security awareness and training?
- Is the board satisfied that the organization has an adequate plan to attract, develop, and retain cyber talent?
- Is the board comfortable that appropriate resources are being invested in the cybersecurity program?

LOOKING AHEAD – CYBER SECURITY'S ROLE IN ONGOING BUSINESS PLANNING PROCESSES

Business plans with fully integrated cybersecurity perspectives have the potential to enable more constructive dialogue in the boardroom. In fact, board members assume that risk insights will inform management's strategic decision making. However, a recent NCS-CIMA study found that less than half of surveyed U.S. organizations considered risk exposures when evaluating possible new strategic initiatives. As a result, strategic bets may not pay off as planned and communications deltas don't diminish.

According to the Gartner CISO Effectiveness Index, top-performing CISOs regularly meet with three times as many non-IT stakeholders as they do IT stakeholders (Gartner Inc., January 28, 2021). That communication has become more important as digital transformation initiatives impact cyber risk profiles and bring increased risk and exposure. Digital transformation initiatives include an expanded use of third parties and a migration to cloud-based platforms, rely heavily on the aggregation and analysis of large amounts of confidential data, and place a premium on speed and flexibility.

Each of these characteristics directly contributes to an increasingly complex cyber risk profile and drives the need for new IT operations and engineering skills to effectively manage cloud environments. Yet, in a 2020 study by CyberGRX and the Ponemon Institute, only 16 percent of respondents said IT security and lines of business are fully aligned with respect to achieving security during the digital transformation process.

Companies have seen their technology ecosystems become far more complex and extend well beyond their traditional network borders. Successful cyber-attacks against SolarWinds and Kaseya illustrate the cyber risk associated with enterprise technology supply chains. Such supply chain events, and the cascading cyber risk associated with them, represent a significant challenge to traditional approaches toward assessing third-party risk. These challenges will increase in the future.

Many organizations are focused on migration to the cloud as part of their digital transformation process. While the infrastructures of the major cloud service providers (CSPs) are much more secure than what most companies can implement in their own data centers, cloud service providers rarely handle all of client's security responsibilities. It's very important that boards understand that however secure cloud service providers may be, organizations never cede accountability for a CSP's failures.

CISOs and the board should review ongoing cybersecurity improvement plans for the security function in the context of the expected evolution of the threat environment and the organization's evolving strategic initiatives.

Questions Boards Should Consider:

- Is the board satisfied with the ways in which the cybersecurity team is engaged in the development of business strategy?
- Is the board satisfied with the ongoing efforts to improve the capability and breadth of the cybersecurity program and how it maintains alignment with both business and technology changes?
- Is the board comfortable that the organization has an effective third-party risk management program that addresses the increasing complexity of the extended enterprise (and the complex outsourcing chains that come with it)?

ABOUT THE AUTHOR

Kevin P. Gowen
Chief Information Security Officer, Synovus Financial

Kevin Gowen serves as Chief Information Security Officer for Synovus and is responsible for all aspects of information and cyber security, physical security, business continuity, fraud, and financial crimes. He was named Chief Information Security Officer in February 2015.

Gowen earned Bachelor's and Master's degrees in Mechanical Engineering from the Georgia Institute of Technology. He received the James H. Blanchard Leadership award in 2016. Gowen was a finalist for both the ISE Southeast Information Security Executive of the Year and the ISE North America Financial Services Information Security Executive of the Year awards in 2019. Gowen is an alumnus of Leadership Columbus and serves as a board member of the National Technology Security Coalition.

WHO WE ARE

The Board Risk Committee (BRC) is a nonprofit, non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG). SFG is a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities, and other critical infrastructure organizations.

Contact:
Catherine A. Allen, Founder, Chairman, Board Risk Committee, cathy@santa-fe-group.com
Ellen Dube, Executive Director, Board Risk Committee, ellen@boardriskcommittee.org