Communicating with the Board about Cybersecurity: Making the Business Case

Cyber risk affects the entire enterprise: it has an impact on business activities at all levels and can be a driver of other significant risks, such as reputational, operational and regulatory risk. An organization's ability to successfully mitigate and respond to cyber risk requires conscientious oversight by the board of directors. Directors, in turn, need senior-level executives to understand and frame this dynamic issue appropriately in order to inform boardroom discussions about cybersecurity. The chief information security officer (CISO) or cybersecurity lead plays a critical role in enabling a strategic approach to cyber risk oversight by the board by providing answers to the right questions and appropriate amounts of data; however, in a National Association of Corporate Directors (NACD) survey, less than 15 percent of directors said they were "very satisfied" with the quality of cybersecurity information they receive from management. This primer, created by the National Cyber Security Alliance (NCSA) and NACD, provides guidelines for effective board-level communication about cybersecurity matters.

What board directors need to know from you about cybersecurity

The role of a board of directors is to provide strategic oversight for the organization and hold management accountable for performance. Management is responsible for execution, including identifying, prioritizing and managing cyber risks. While the specific information your board needs will vary depending upon the organization's industry, regulatory requirements, operating activities, geographic footprint and risk profile, all boards are looking to management to translate technical, tactical details about cybersecurity into business terms: risks, opportunities and strategic implications. Board members are asking CISOs the following questions about cybersecurity:

1. What is our cyber risk appetite?
2. What are the most important metrics we use to monitor and evaluate risk to the company?
3. What is the business case for cybersecurity? How can cybersecurity enable other business functions across the enterprise?
4. What are the levels of insider and outsider risk?
5. How do we measure the effectiveness of our organization's cybersecurity program and how it compares to those of other companies? For example, how do we track cybersecurity awareness across the organization through indicators such as policy compliance, implementation and completion of training programs?
6. How do we assess the cyber risk position of our suppliers, vendors, joint venture partners and customers?

Source: Adapted from NACD Director's Handbook on Cyber-Risk Oversight

7. How much of our IT budget is being spent on cybersecurity-related activities? How does this allocation compare to those of our competitors/peers and/or to other outside benchmarks?
8. How many data incidents has the organization experienced in the last reporting period? What are the important trends, patterns and root causes?
9. What are the breadth and depth of the company's operational cybersecurity monitoring activities? Are there areas we are not monitoring, and if so, why not?

Guiding principles for providing board-level metrics

After you have considered what your board needs to know about cybersecurity, you will need to convey key takeaways with supporting data. Board members are looking for insight on the state of the organization's cybersecurity program and the business implications of cyber risks; they do not want large amounts of technical detail or operational, compliance-oriented metrics.

Keep the following guiding principles in mind when preparing board-level reports:

1. Make sure the data is relevant to the organization's business context and can be understood by the audience.
2. Be concise: Avoid providing too much information, and eliminate technical jargon.
3. Less is more: Minimize text, and include graphics and visuals to convey your key points.
4. Communicate insights about what the data means, not just information. Metrics should include analysis of changes, trends and patterns over time, show relative performance and indicate impact.
5. Above all, board-level reports should enable strategic discussion and dialogue between directors and senior management.

Source: NACD Director's Handbook on Cyber-Risk Oversight

NACD's Director's Handbook on Cyber-Risk Oversight and online Cyber-Risk Oversight Course have more information about effective board management communications on cybersecurity matters; visit nacdonline.org/cyber to learn more.

Additional Resources:

- NCSA's CyberSecure My Business: https://staysafeonline.org/cybersecure-business/
- National Institute of Standards and Technology Cybersecurity Framework: https://www.nist.gov/cyberframework

NATIONAL CYBERSECURITY ALLIANCE

NACD®