CYBER-RISK OVERSIGHT

How Internal Audit Helps Increase Cybersecurity Transparency for the Board

By John Brackett and Ken Stasiak

Cybersecurity and data privacy issues continue to make headlines, and the risks surrounding them are only increasing. The demands on chief information security officers and chief technology officers expand as data moves from in-house systems to cloud computing, mobile devices, remote work setups, and new technologies including artificial intelligence and robotic process automation. As security and privacy risks increase, a disconnect between security personnel and the board could leave the organization more vulnerable.

To avoid this disconnect, the board should make a concerted effort to maintain an accurate picture of the risk profile of the organization and the strength of its cybersecurity program. Despite the intricacies of managing emerging technologies, security and privacy risks, and compliance requirements, executives' confidence in their cybersecurity programs remains high. In RSM's *Cybersecurity Special Report*, 93 percent of C-suite respondents expressed confidence that current safeguards protect their organizations' data. Considering the increased disruption, threats, and compliance burdens, boards should reevaluate their confidence levels and ensure that management's perceptions of security remain realistic.

AN INCOMPLETE PICTURE OF ENTERPRISE RISKS

To make data actionable, board members are often presented with high-level summaries that provide snapshots but may not capture the true nature, extent, and urgency of security, privacy, and compliance risks. Filtering the information in this way may dilute the perception of their severity. Thus, boards are making decisions without an accurate and complete picture of the risk profile.

A lack of security resources also may result in an incomplete picture of security and privacy risks for the board, caused by, and in turn causing, reduced communication with security personnel. As the demand for cybersecurity resources outpaces supply, and as cyber risks grow in number and become more severe, even organizations with standard security resources may not have a direct line of communication with the decision-makers. Furthermore, a lack of trust exacerbates this information gap between technology personnel and the board.

HOW INTERNAL AUDIT CAN HELP

The internal audit committee can play a key role in overseeing security, privacy, and compliance by offering an effective approach to identifying, communicating, and managing risks. Internal audit's mission is to enhance and protect organizational value by providing risk-based guidance. Internal audit can partner with cybersecurity teams to sponsor in-depth assessments that exhance visibility of cybersecurity risks.

Moreover, while cybersecurity teams may not frequently interact with the board, internal audit often has a direct line of communication to directors. Connecting cybersecurity with internal audit can better elevate risks to executives and the board, reduce information filtering, and promote improved collaboration.

THREE KEY TAKEAWAYS FOR BOARD MEMBERS

1. Board members may ask management to perform a cybersecurity assessment, but such requests are often ambiguous. Cybersecurity or information technology (IT) professionals may interpret these requests without fully understanding the board's intent, resulting in assessments that do not provide the visibility the board had anticipated. If possible, correlate the request to specific concerns (e.g., ransomware or overall program maturity).

2. Ask internal audit to participate in the cybersecurity assessment(s). Getting internal audit involved will allow for greater transparency of the findings while providing a path to fully communicate the cyber risks to the board.

3. Ensure that there is a cybersecurity steering committee that meets on a regular basis to discuss cyber risks. This committee should determine how and when to present to the board. Involving business units and functions outside of IT and cybersecurity in this committee will facilitate broader discussions, help articulate the business impact of cyber risks, and tie cyber risks to enterprise risk management strategies. D

John Brackett (*left*) leads RSM's risk advisory consulting practice. Ken Stasiak is a leader in RSM's security and privacy risk consulting practice.