The board convened to discuss critical aspects of cybersecurity, focusing on communication, supply chain risk management, and incident response preparedness. The discussion centered around three key principles: planning, implementation, and incident response.

Communication Channels

The board emphasized the importance of establishing uniform cybersecurity communication channels across all subsidiaries. They explored strategies to accelerate the rollout of these pathways before the end of 2025[1](https://www.irmi.com/articles/expert-commentary/communication-during-cyber-attacks-and-data-breaches). A key concern was addressing the reluctance of suppliers and third parties to share cybersecurity risk information. The board considered implementing secure, automated reporting mechanisms to alleviate this reluctance and facilitate more open communication[2](https://securityscorecard.com/platform/third-party-cyber-risk-management/).

Supply Chain Risk Management

The discussion then shifted to integrating cybersecurity supply chain risk management into the broader enterprise risk management framework. The board recognized the need to expand their strategy beyond U.S. suppliers to encompass a global approach[5](https://www.bluevoyant.com/knowledge-center/third-party-risk-management-tprm-a-complete-guide). They also discussed best practices for seamlessly integrating cybersecurity risk into enterprise risk management frameworks. A crucial point was raised about educating board members to recognize cybersecurity as a critical element of enterprise-wide risk, rather than a purely technical issue[2](https://securityscorecard.com/platform/third-party-cyber-risk-management/).

Incident Response Preparedness

The board acknowledged the importance of regular practice sessions to prepare for potential cyber events. They discussed methodologies to improve their ability to anticipate cyber incidents despite their unpredictable nature[1](https://www.irmi.com/articles/expert-commentary/communication-during-cyber-attacks-and-data-breaches). The board explored ways to foster collaboration between staff and board members to finalize a cohesive incident response framework. They also considered measures to ensure real-time data accessibility across all necessary business units to enhance enterprise-wide cyber preparedness[6](https://www.eccu.edu/blog/how-to-effectively-communicate-cybersecurity-best-practices/).

Throughout the discussion, the board emphasized the need for clear, consistent communication and collaboration in addressing cybersecurity challenges[6](https://www.eccu.edu/blog/how-to-effectively-communicate-cybersecurity-best-practices/). They recognized the importance of simplifying technical jargon and speaking in plain language to ensure all stakeholders understand the risks and mitigation strategies[8](https://www.connectwise.com/resources/msp-cybersecurity-challenges/ch6-client-communication). The board also highlighted the need for a balanced approach when communicating about risks and threats, grounding all communications in facts while providing potential solutions to instill confidence[8](https://www.connectwise.com/resources/msp-cybersecurity-challenges/ch6-client-communication).