A Board Member's Quick Reference Guide:

1. Where is AI truly being used across our company, and by whom?
2. How are we guaranteeing our proprietary or sensitive data cannot be accidentally exposed by any AI system?
3. Are we developing our AI solutions with security guardrails as foundational elements?
4. Who or what is truly in charge of our AI's actions, and can we instantly stop it if something goes wrong?
5. Are our existing cybersecurity solutions creating a "time tax" that slows down our AI initiatives?
6. Do we have the cybersecurity resources (human and machine) to match our new AI ambitions?
7. When AI goes rogue, how quickly can we recover, and are we covered by insurance?
8. How are we ensuring our AI systems are fair, transparent, and free from hidden biases that could harm our customers, employees, or reputation?
9. Are we implicitly trusting third-party AI platforms or open-source components with our AI risks?
10. Do we have a clear AI roadmap and the right oversight to navigate this new era?