blackwell

~290 Days
average recovery time from a ransomware incident

> $ 100 B
losses estimated due to cyber incidents in US healthcare

$ 10.1 M
Average Cost of a healthcare data breach

10 Questions Healthcare Boards Need To Be Asking About Cybersecurity

And key indicators for any Board responsible for protecting PHI and Patient Care.

The rise in malicious attacks and data breaches has shown just how brittle the US healthcare industry has become. Cybersecurity has become a top five concern for Boards of Directors and is quickly moving higher in the wake of the 2024 Change Healthcare and Ascension ransomware attacks.

Below are ten questions board members should ask their healthcare companies about cybersecurity during board meetings to understand the robustness of the cybersecurity measures and risk management.

> ***"It is essential for boards to continuously incorporate cyber risk management discussions related to the most effective way to reduce the financial and business impact connected with cyber risk. (...) It's a broader c-suite discussion."***
>
> - Chris Hetner, Nasdaq Center for Board Excellence Insights Council member

250-1000x
Medical Record value compared to SSN on the Black Market

~35%
breaches attributed to 3rd Party Risk

10-15
Security Staff needed for Medium-sized Health Systems

Questions for Board Governance Over Cybersecurity

1. **Does the Board of Directors regularly review Cybersecurity Performance?** Including cybersecurity regularly on the board agenda helps align business and cybersecurity objectives and ensures regular operational review.

2. **Do board reports communicate accepted Cybersecurity risks?** - Board reports should focus on understanding both accepted cyber risks and exceptions granted to cybersecurity policies and controls, as permitted cyber risks multiply the overall risks of doing business.

3. **Is Cybersecurity Governance under committee or direct board review?** Audit and Compliance Committees can help boards perform deeper governance and review of cybersecurity programs. However, it can also distance boards from fully understanding the likelihood and impact of a cyber attack on the business. Ensure that reporting cadence and depth align for comprehensive oversight that is right for the business.

Questions for the CEO and Company Leadership

4. **What is our overall cybersecurity strategy, and how does it align with our organizational goals?** - Signals of a comprehensive strategy include: 1) Alignment to business goals, 2) use of a standard framework (NIST, SOC 2, HITRUST, etc), and 3) benchmarking performance year-to-year and against similar companies.

5. **How frequently do we conduct cybersecurity risk assessments, and what have been the key findings from recent assessments?** - Elements of healthy risk assessment practices include 1) specialized risk assessments throughout the year, 2) risk assessment built into business and technology change processes, and 3) external assessments to validate internal assessments and find blind areas.

6. **What is our operating and governance structure for cybersecurity, and how is the board kept informed about cybersecurity issues and developments?** Day-to-day and leadership cybersecurity responsibilities may operate at several levels under C-Suite leadership. Regardless of the operating structure, the CEO must ensure unbiased assessments of cybersecurity performance are delivered to the leadership team and the Board of Directors.

The blackwell Difference

Breadth of Technology Integrations

PHI Data Detection & Response Handling

Healthcare Tailored Playbooks

Fully US-based, expert Security Team

Cybersecurity Operations Performance Questions

7. **What are the most significant cybersecurity threats and vulnerabilities we face, and how are we addressing them?** - Signals of mature threat assessment include: 1) frequent scanning (ideally weekly or daily) for new vulnerabilities, 2) proactive threat hunting, and 3) awareness of new threats and issues in the industry.

8. **How do we handle incident response, and what is our plan for managing and recovering from a ransomware attack or data breach?** - Key indicators of a comprehensive plan should include; identification of critical systems, response speed objectives, org-wide communication plans, recovery time objectives, downtime procedures, and regular tabletop simulation testing and improvements.

9. **What measures are in place to protect patient data and ensure compliance with regulations such as HIPAA?** - A multi-layered, or secure-by-design, approach should be in place. Protection methods should be in place for the system of record, and as data moves across the organization and between third parties. Measures should include MFA, backups and encryption, role-based access, patching, and network segmentation at a minimum.

10. **What technologies and methods are we using to monitor and defend against internal and external cyber threats, and how do we check for gaps in monitoring?** - The right mix of threat detection technologies will depend on the size of the company and the complexity of the operational technology in use.
    - At a minimum protecting PHI and patient care should include:
        - 24x7 active monitoring and threat hunting by a Security Operations team or vendor
        - Endpoint, Network, Cloud, Application, Email, and User-based detection and response technologies
        - Data Protection and Data Loss Prevention to detect data leaks
        - Automation and AI to speed up response and automatically block attacks