The Cyber Attack Prevention Checklist

HOW TO PREPARE YOUR BOARD AND LEADERSHIP TEAM

A best practice approach to helping healthcare providers protect their digital infrastructure requires involvement from your organization's board and C-suite. Without guidance and an orchestration across people, processes and technologies, even the best strategy may not reach its full potential. Here are seven critical factors that will guide your board and executive team to a more effective and successful cyber risk framework:

01

Know Your Place

There's no one-size-fits-all template for cybersecurity. It's critical to tailor a program to your organization's specific needs. This means adapting and tweaking policies, practices and technologies to align with your healthcare organization's company and culture.

02

Know Your Stuff

The board and CEO can no longer assign all cybersecurity responsibilities to the Chief Information Security Officer (CISO). It's essential that the board has a foundational understanding of cyber risk, and patient data breach, and one or two board members possess deeper knowledge. The inability to ask the right questions may increase risk.

03

Know More

Board members should make a point to read about cybersecurity and attend workshops and training sessions to learn about the latest trends and developments. For example, analytics, artificial intelligence (AI) and other technologies are changing the face of cybersecurity, which could ultimately impact your organization's risk mitigation strategy.

04

Oversight Is Everything

It's critical to establish a cyber risk committee, task force or team to serve as an intermediary between the board and the rest of your organization. This group should report to the board on a regular basis.

05

Think Beyond Auditing

It's wise to have an audit committee in place to identify gaps, problems and success stories. However, this committee should never be charged with fixing problems. It's critical to set up a separate cybersecurity committee to identify technologies and processes that mitigate risk.

06

Governance Can't Be Ignored

Establishing an effective governance framework is paramount. It will help you hardwire policies and procedures into the organization, while ensuring that units, departments and teams have the flexibility and autonomy they need to complete their work.

07

Communication Is Critical

A board requires a safe and secure place to interact and exchange messages, files and documents. Nasdaq Boardvantage is a dedicated board portal that can support your organization. As a communication and collaboration space, it uses a privilege-based model to support interactions with CSOs, CISOs and other executives with specific cyber risk responsibilities.

Within the next year, 85% of organizations plan to implement board and CEO involvement in cybersecurity,[1] and 90% expect investments in cybersecurity to grow over the next three years.[2]

A best practice model can significantly improve an organization's cyber risk framework. Will your organization be one of them?

For more information about the board and C-suite's growing role in managing cyber risk, download our eBook,

Best Practices in Cyber Risk Governance

[1] Ponemon Institute, "The Third Annual Study on the Cyber Resilient Organization," March 2018.
[2] Accenture, "Gaining ground on the cyber attacker," 2018.