Cybersecurity Cheat Sheet for the Board of Directors

What You Need to Know: A Starter Guide to Find and Fulfil Your Role in Cybersecurity

Amidst health care transformation, complicated federal regulation, margin pressures, and the push to innovate, adding the complex topic of cybersecurity to executive plates is understandably overwhelming. But the task of ensuring effective management of cyber risk falls to senior leadership. Examples from both inside and outside of health care clearly illustrate that organisations can delegate day-to-day security responsibility to IT and security leaders, but ultimate accountability for cyber risk lies with senior leaders across the entire enterprise.

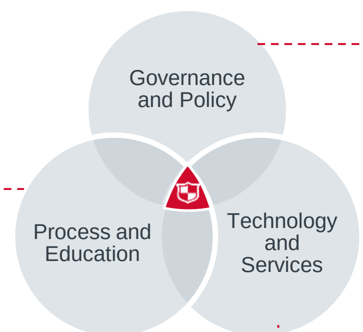
A Comprehensive Approach to Cybersecurity

When an incident occurs, all departments, all staff, and even patients can be impacted. Senior leadership must act to ensure effective prevention and response through a comprehensive approach that reaches well beyond technology. Below is our cybersecurity ecosystem model with three layers: governance and policy; process and education; and technology and services. A weakness in any of these areas will limit the effectiveness of the others. Building cyber resilience requires organisation-wide investment through time, attention, and funding across all three layers.

The Cybersecurity Ecosystem

Process and Education

- Training and testing
- Incident response planning
- Audits
- Risk assessments
- Business continuity planning, disaster recovery, and back-ups



Governance and Policy

- C-suite and board engagement
- Dashboards
- Governance
- Standards
- Strategy
- Staffing
- Digital trading partners

Technology and Services

- Cyber intelligence
- IT-enabled capabilities
- Cyber insurance
- Information sharing

Why Does the Board Need to Be Involved in Cybersecurity Issues?

Boards play a crucial role in cyber risk that goes beyond mere compliance tracking: they must set an acceptable level of risk for the organisation and ensure that executive management mitigates cyber risk to that level. In the end, boards must be willing to stand behind the security programme its management team enacts. This requires that boards:

- Establish an appropriate level of cybersecurity oversight which enables them to understand and track enterprise risk and remediation efforts
- Require continuing education and briefings for board members on new and emerging threats to the organisation
- Regularly review the collective experience and skills of the board in regard to cybersecurity and technology to ensure the board has members with an appropriate background for guiding management in security matters

Critical Questions Board of Directors Should Ask About Cybersecurity

Boards should be proactive and request a briefing with management to share the board members' general attitude about risk and security; their level of cybersecurity knowledge (you are not expected to be experts); and their underlying concerns around risk and security. This will help your security leaders craft presentations and viable security alternatives that will be meaningful to the board.

The complex nature of cybersecurity and the rapid escalation of threats can make it hard to know where to focus. Below are questions board members may find useful to reflect upon their own engagement in cybersecurity or to partner with the organisation's security leader to answer and resolve. Questions and subsequent actions should address all layers of the ecosystem. Space to draft your own questions is provided.

Governance and Policy	❑ What role does the board have or want in cybersecurity? ❑ Has the board established a clear objective for cybersecurity risk? Is there agreement on an acceptable level of risk to take on? ❑ Has management developed and implemented a security programme that the board can stand behind? ❑ Does your security program include elements from recognised security standards such as ISO or NIST?[1] ❑ What mechanisms are in place to track security status and progress? ❑ Is there a thorough information security due diligence analysis performed prior to mergers, acquisitions, partnerships, and alliances? ❑ How is risk from third-party arrangements managed on an ongoing basis? Is it approached as a continuous process? ❑ ______________________
Process and Education	❑ Is there a security awareness training programme in place? ❑ Does the board receive frequent and regular updates on evolving threats? ❑ Is an incident response plan in place? Is it tested? ❑ Are business continuity plans in place? Are they up to date and tested across all shifts? ❑ ______________________ ❑ ______________________
Technology and Services	❑ Is management tracking the latest technologies for cybersecurity? ❑ ______________________ ❑ ______________________

1) ISO = International Organization for Standardization; NIST = National Institute for Standards and Technology.

Advisory Board

Third Floor, Melbourne House, 46 Aldwych, London WC2B 4LL, UK
P +44 (0) 203 100 6800 | F +44 (0) 203 318 3069 | **advisory.com**