Cybersecurity Cheat Sheet for the Chief Executive Officer

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

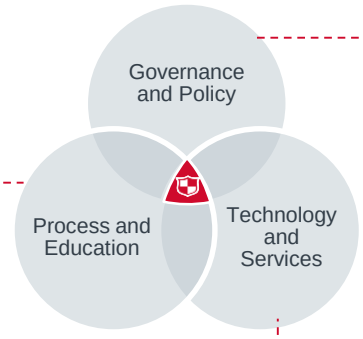
Amidst health care transformation, complicated federal regulation, margin pressures, and the push to innovate, adding the complex topic of cybersecurity to executive plates is understandably overwhelming. But the task of ensuring effective management of cyber risk falls to senior leadership. Examples 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 CEO Need to Be Involved in Cybersecurity Issues?

Cyber incidents can put an institution's ability to fulfil its mission to care for its patients and community at risk, so it is vital that CEOs ensure such risks are managed effectively. Beyond the potential for significant operational disruption, organisations face hefty costs and fines that easily stretch into the millions of dollars, and lasting reputational damage that may impact potential mergers, acquisitions, and partnerships. Additionally, CEOs and other C-suite executives may be held personally liable for the consequences of a cyber incident if they cannot demonstrate appropriate efforts at mitigation. CEOs have a responsibility to lead the institution in a positive security-focused culture, fostering an environment that engages all personnel and leadership. Key actions include demanding inclusive and thorough security governance and oversight; setting expectations for improvement in end-user training, testing, and preparedness; and not pointing fingers when an incident occurs. On the technology side, CEOs should focus not on understanding technical details of investments or specific ROI,[1] but on ensuring the organisation sees value from each.

1) ROI = Return on investment.

Critical Questions CEOs Should Ask About Cybersecurity

CEOs should proactively engage with both their board and leadership team on security issues and initiate a discussion with the board on security to establish their oversight role. Security must have a regular place on C-suite agendas. CEOs should ensure that all C-suite members have a clearly defined role and accountabilities for security matters. These critical questions will get you started—they should facilitate, not replace, an in-depth conversation with the security leader.

The complex nature of cybersecurity and the rapid escalation of threats can make it hard to know where to focus. Below are questions CEOs may find useful to reflect upon regarding their engagement in cybersecurity, and 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

- ❑ Does the security governance structure engage all levels of leadership and enable staff to have a voice in decisions impacting their work?
- ❑ Is there a security strategy in place? Does it support the organisational strategy?
- ❑ Do you track progress according to a meaningful security dashboard that provides actionable information for making key decisions?
- ❑ To whom does the security officer report? Are they empowered with the authority required to make progress in the organisation's security posture?
- ❑ Who has the final say on risk assessments?
- ❑ Is there a continuous third-party risk management process in place?
- ❑ Do you include cybersecurity in due diligence of M&A[2] and partnership activities?
- ❑ _____

Process and Education

- ❑ Are executive-level security awareness training and testing in place? Are all executives included and required to take any necessary remediation training?
- ❑ Are robust security awareness training and frequent testing in place for all employees? Do you track testing results regularly? Do you see improvement over time? Are business leaders (not just IT) held responsible for improvement?
- ❑ Is there an incident response plan in place? Is it regularly tested? Are key personnel imbued with authority to make decisions in a time of crisis?
- ❑ What is your Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for your disaster recovery plans?
- ❑ _____

Technology and Services

- ❑ Are basic technologies such as encryption, mobile device management, and intrusion detection in place prior to investing in more complex security technologies?
- ❑ Do your security technology investments support the overall security strategy?
- ❑ _____

2) M&A = Mergers and acquisitions.

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**