Cybersecurity Cheat Sheet for the Chief Medical or Nursing 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.

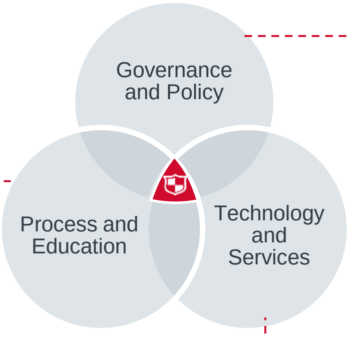
A Comprehensive Approach to Cybersecurity

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 CMO or CNO Need to Be Involved in Cybersecurity Issues?

For CMOs and CNOs, cybersecurity is primarily a safe patient care and clinician workflow issue. The May 2017 WannaCry attack forced several health systems in England to turn away patients and cancel droves of appointments and surgeries while IT systems were down. You and your clinicians across the enterprise must be ready to safely care for patients in the absence of the critical information systems to which we have grown accustomed. From a workflow perspective, clinicians log into systems 50–100 times a day, so security controls can acutely impact this population—you have likely fielded their concerns and you will need to be able to explain why these controls are necessary, setting a positive attitude toward security. CMOs and CNOs can vocalise clinician concerns as the organisation designs its security plan, and hold staff accountable for performance in the event of a crisis.

Critical Questions CMOs or CNOs Should Ask About Cybersecurity

The CMO and CNO need to set the tone for clinical staff. They can make it clear that maintaining security is an important aspect of clinical practice and lead by helping to establish reasonable and responsible security controls in partnership with the CIO and the security officer. 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 CMOs and CNOs 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

- ❑ Is there a clinical voice in the organisation's security governance structure? If not, how can you incorporate the clinical perspective into planning and oversight to ensure workflow and other concerns are considered?
- ❑ Do clinicians view security measures as *assurance* (e.g., protecting patients and the organisation) or *hindrance* (e.g., gets in the way of their daily work)?
  - ❑ What are specific clinician concerns or misconceptions about security?
  - ❑ How can you support activities that foster a positive view of security?
- ❑ Are clinicians involved in the review and testing of new policies and procedures to provide feedback?
- ❑ Have you developed a robust explanation for why security controls are so important and how to use them effectively?
- ❑ ____

Process and Education

- ❑ Do your downtime procedures incorporate security incident scenarios? Are detailed processes in place to ensure continued safe patient care?
- ❑ Are clinical staff regularly trained and tested on security awareness?
  - ❑ What is your approach for dealing with doctor or nurse repeat offenders?
- ❑ Are clinicians involved in the review and testing of new policies and procedures to provide feedback?
- ❑ Are all shifts of clinicians adequately prepared to enact business continuity procedures should the need arise? Are new hires trained during onboarding?
- ❑ Are clinical staff knowledgeable of what to do in the first few moments when they suspect an incident or attack has started?
- ❑ Do clinicians understand the role incident response teams play during events?
- ❑ ____

Technology and Services

- ❑ How are clinical workflow needs taken into consideration when weighing potential new security tools and services?
- ❑ ____