Cybersecurity Cheat Sheet for the CMIO or CNIO

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.

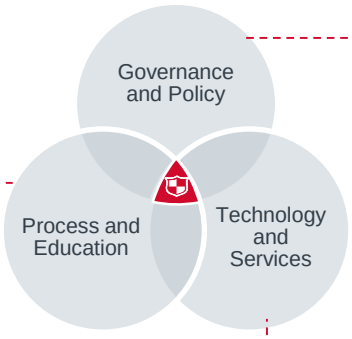
A Comprehensive Approach to Cybersecurity

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 CMIO or CNIO Need to Be Involved in Cybersecurity Issues?

CMIOs and CNIOs are critical partners for security teams. Not only does your role bring a clinical perspective to the leadership team, but you can effectively translate technical IT and security concepts into terms that clinicians understand. CMIOs and CNIOs must engage in cybersecurity for three main reasons:

- Clinicians will come to you—perhaps frustrated with security controls—and you will need to be able to educate them and address their concerns.
- You need to be involved in the planning and design of the security programme to ensure the development of a practical approach that will permit successful clinician adoption.
- You have a critical role in preparing clinicians to continue to practice following a security breach, when the EMR and other clinical systems may be off-line.

Critical Questions CMIOs or CNIOs Should Ask About Cybersecurity

CMIOs and CNIOs should proactively engage with clinical staff throughout the enterprise on security issues. Consequently, he or she should initiate discussions with the security officer and CIO to establish his or her role in cybersecurity, ensure they have answers for clinician concerns, and define a place at the table for decisions that impact clinical work. 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 CMIOs and CNIOs 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

- ❑ Do you take part in security governance and planning conversations? Is a clinical voice incorporated in some way to ensure clinicians' concerns are considered?
- ❑ Do clinicians view security measures as an *assurance* (e.g., a way to protect patients and the organisation) or a *hindrance* (e.g., gets in the way of daily work)?
    - ❑ How can you support activities that foster a positive view of security?
    - ❑ Have you developed a robust explanation for why security controls are so important and how to use them effectively?
- ❑ What are specific clinician concerns or misconceptions about cybersecurity?
- ❑ Do you currently include regular discussion about security threats, the severity of security risks, and security-related workflow impacts in your communications with clinicians?
- ❑ Are you working regularly with security leaders?
- ❑ _____

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?
- ❑ _____

Technology and Services

- ❑ How are clinical workflow needs and current risky practices (such as unsecure provider-to-provider communication) weighed when considering potential new security tools and services?
- ❑ _____

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**