Advisory Board | International
Global eHealth Executive Council

The best practices are the ones that work for **you.**SM

Cybersecurity Cheat Sheet for the Chief Legal Counsel

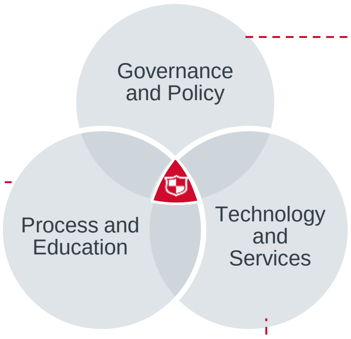
What You Need to Know: A Starter Guide to Find and Fulfil Your Role in Cybersecurity

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 Chief Legal Counsel Need to Be Involved in Cybersecurity Issues?

Addressing cyber risk effectively is vital for the institution's ability to fulfil its mission to care for its patients and community. It is much broader than a compliance issue. Security teams cannot eliminate all cyber risk—but they can leverage the elements of the cybersecurity ecosystem to mitigate the risk to an acceptable level. In addition to a personal liability, cyber incidents can bring significant operational disruption, hefty costs and fines that easily stretch into the millions of dollars, governmental scrutiny, and lasting reputational damage that may impact M&A[1] and partnerships. Many countries initiate in-depth investigations following any breach of patient data, so organisations must be able to demonstrate that they not only had policies documented, but that they were practiced and any shortcomings were addressed once identified.

[1] M&A = Mergers and acquisitions.

Critical Questions Chief Legal Counsel Should Ask About Cybersecurity

Legal Counsel must treat security as more than a compliance issue. Significant risk to business and operations can exist even in organisations that are compliant with all regulatory and contractual requirements. Legal Counsels should engage their security officer and CIO to ensure that the organisation has adequate policies in place to address such issues as data classification, data handling, retention, and access. They can ensure that all third-party arrangements have clearly defined expectations and responsibilities which are understood by senior leaders. Preparations to meet e-discovery requirements should be led and supported by the legal department.

The complex nature of cybersecurity and the rapid escalation of threats can make it hard to know where to focus. Below are questions the Chief Legal Counsel may find useful to reflect upon his or her 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

- ❑ Are security policies consistently enforced and backed by appropriate and acceptable disciplinary actions? How will the organisation handle clinician or executive "offenders"?
- ❑ Is the legal perspective included in the security governance? Does the governance structure demonstrate effective oversight?
- ❑ Are key security policies in place, such as the definition of the legal medical record?
- ❑ Are there clear and comprehensive security agreements with digital trading partners that clearly articulate each party's role and expectation in the event of a breach?
  - ❑ Are these updated over time as the nature of the relationship changes?
  - ❑ Are all contractual obligations of the enterprise documented and clearly understood by senior leaders?
- ❑ Are various audit efforts (IT, security, financial, internal) across the organisation aligned so that they can share information and support each others' efforts?
- ❑ ____

Process and Education

- ❑ Are mechanisms in place to monitor and document security training?
- ❑ Does the organisation have a thoroughly vetted breach plan ready to swiftly activate in the event of a cyber incident?
- ❑ After incidents, does the organisation conduct post mortem reviews to document and learn from what happened and take action to improve?
- ❑ ____

Technology and Services

- ❑ Can you isolate and freeze data and documents potentially subject to e-discovery?
- ❑ Are liabilities clear in contracts with third-party service providers?
- ❑ Are third-party service providers compliant with all regulations that apply to your organisation?
- ❑ ____