Cybersecurity Cheat Sheet for the Chief Financial Officer

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

Amidst health care transformation, complicated governmental regulations, 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.

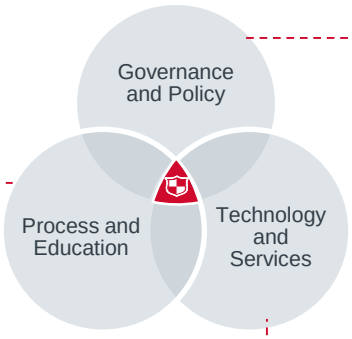
A Comprehensive Approach to Cybersecurity

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 CFO 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. Cyber incidents now have significant financial ramifications that can derail carefully managed budgets. On top of hefty clean-up costs, some governments now levy substantial fines. By nature, it can be difficult to demonstrate strong ROI[1] for security investments—what is the cost of an event that did not happen? Instead, CFOs should ensure the organisation has adequate funding to advance to the desired security maturity level, that funds are set aside to use during incident response, and that the organisation sees value and impact from the investments it does make.

1) ROI = Return on investment.

Critical Questions CFOs Should Ask About Cybersecurity

CFOs must recognise that security is more than just an audit issue and that serious financial and even personal liability can result from security incidents. CFOs should engage their security officer and CIO to ensure that the organisation gets the best return on its security technology investment by lending their personal support to matching governance and process measures. In addition to providing funding for staffing and technology, CFOs can be a powerful voice in favour of such valuable mitigations as third-party risk management, staff training and testing, and business continuity planning.

The complex nature of cybersecurity and the rapid escalation of threats can make it hard to know where to focus. Below are questions CFOs 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

- ❑ Are security financial risks understood and enumerated?
- ❑ Are budgetary resources available for security governance to allocate?
- ❑ Who manages the security budget?
- ❑ Is adequate funding available to support the organisation in its planned security initiatives?
- ❑ Is adequate funding available to meet security staffing and hiring needs in the current security talent market?
- ❑ Is risk from third parties regularly reviewed and mitigated?
- ❑ _____

Process and Education

- ❑ Are reserves set aside for incident response? Are financial resources available and accessible to incident response teams during crises?
- ❑ Do employees (including executives) with access to funds receive tailored security awareness training on a regular basis? Are they regularly tested?
- ❑ Are business unit leaders held accountable for establishing effective business continuity plans?
- ❑ Is there a well maintained centralised repository of security gaps and mitigation plans that includes the findings from internal and external audits, as well as from risk assessments and penetration tests?
- ❑ _____

Technology and Services

- ❑ Are funding requests for security tools and services vetted against a security strategy and roadmap?
- ❑ Do you have cyber insurance? If so, do you understand what is and is not covered under your specific cyber insurance plan?
- ❑ Are regular penetration tests and risk assessments funded and performed?
- ❑ _____

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**