Cybersecurity Cheat Sheet for the Chief of Human Resources

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.

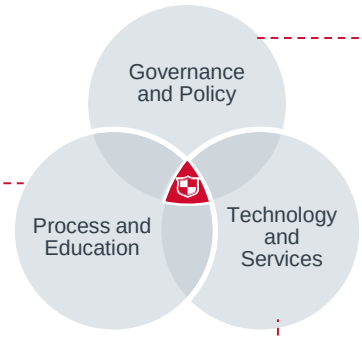
A Comprehensive Approach to Cybersecurity

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 of HR Need to Be Involved in Cybersecurity Issues?

Many elements of the cybersecurity ecosystem, especially those under the “Governance and Policy” and “Process and Education” layers, rely heavily on employee understanding and participation. The rising operational and financial stakes of cyber incidents pose a greater need to hold individuals accountable for patterns of behaviour (such as repeated failings of internal phishing tests) that bring great risk to the institution. The Chief of HR is a critical partner in the development, roll out, and enforcement of any security accountability programme. Some organisations now include security competencies in performance reviews to signal the expectation of positive security behaviour. With staffing, the information security talent market is tough, with no signs of easing. Recruitment and retention of talented, experienced security staff—especially the CISO—may require special attention to ensure the organisation has the talent to operationalise its security strategy.

Critical Questions the Chief of HR Should Ask About Cybersecurity

The Chief of HR should proactively engage with senior leaders throughout the enterprise on security issues. Human Resources can facilitate, track, and document staff training and education on policies and obligations. They should also ensure efficient processes are in place to notify security operations of staff changes that may impact access controls. HR also has a unique role in working with the CIO and security officer to ensure employee data is appropriately protected.

The complex nature of cybersecurity and the rapid escalation of threats can make it hard to know where to focus. Below are questions Chiefs of HR 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 policies consistently enforced throughout the organisation?
- ❑ Does the security team have the necessary staff to operationalise the security strategy or make the necessary progress in the expected time frame?
- ❑ Does the CISO hiring process ensure compatibility and support from key executive leaders (especially the CEO, CFO, CMO, and CIO)?
- ❑ What efforts are in place to retain existing security talent?
- ❑ Have you considered alternative staffing sources such as growing talent and expertise from within, out-of-industry recruitment strategies, virtual or outsourcing options, university partnerships, and veteran talent pools?
- ❑ Could IT and security managers benefit from additional or customised workforce management training (e.g., how to spot burn out, staff engagement, effective feedback delivery, retention conversations)?
- ❑ _____

Process and Education

- ❑ Are employee expectations codified in firm policy? Is there appropriate documentation of staff training on security policies and obligations? Are all staff regularly trained and tested on their security obligations?
- ❑ How will your organisation hold employees accountable? Does the accountability structure fit the culture of the organisation? Are legal, compliance, and IT/security leaders in agreement? How will you handle clinician or executive offenders?
- ❑ Should the organisation include an element of cybersecurity in its performance reviews? If so, how (e.g., merit increases released only after any outstanding training is completed)?
- ❑ What can be done to proactively avoid some potential negative situations, such as eliminating external email access for employees for whom it is not core to their role?
- ❑ Have processes been put in place to ensure timely notification of job changes so access can be adjusted appropriately?
- ❑ _____

Technology and Services

- ❑ Is appropriate security and IT talent in place to get the most value from technical investments?
- ❑ How will skill needs change based on planned technical investments on the security roadmap?
- ❑ Are adequate protections in place for the organisation's employee data?

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**