Cybersecurity Cheat Sheet for the Board of Directors

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.

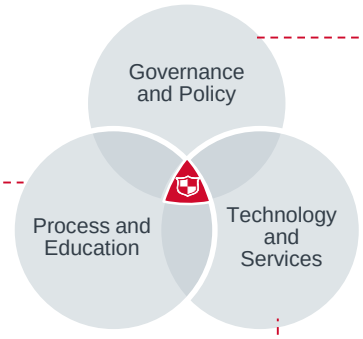
A Comprehensive Approach to Cybersecurity

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 Board Need to Be Involved in Cybersecurity Issues?

Boards play a crucial role in cyber risk that goes beyond mere compliance tracking: they must set an acceptable level of risk for the organisation and ensure that executive management mitigates cyber risk to that level. In the end, boards must be willing to stand behind the security programme its management team enacts. This requires that boards:

- Establish an appropriate level of cybersecurity oversight which enables them to understand and track enterprise risk and remediation efforts
- Require continuing education and briefings for board members on new and emerging threats to the organisation
- Regularly review the collective experience and skills of the board in regard to cybersecurity and technology to ensure the board has members with an appropriate background for guiding management in security matters

Critical Questions Board of Directors Should Ask About Cybersecurity

Boards should be proactive and request a briefing with management to share the board members' general attitude about risk and security; their level of cybersecurity knowledge (you are not expected to be experts); and their underlying concerns around risk and security. This will help your security leaders craft presentations and viable security alternatives that will be meaningful to the board.

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

- ❑ What role does the board have or want in cybersecurity?
- ❑ Has the board established a clear objective for cybersecurity risk? Is there agreement on an acceptable level of risk to take on?
- ❑ Has management developed and implemented a security programme that the board can stand behind?
- ❑ Does your security program include elements from recognised security standards such as ISO or NIST?[1]
- ❑ What mechanisms are in place to track security status and progress?
- ❑ Is there a thorough information security due diligence analysis performed prior to mergers, acquisitions, partnerships, and alliances?
- ❑ How is risk from third-party arrangements managed on an ongoing basis? Is it approached as a continuous process?
- ❑ _____

Process and Education

- ❑ Is there a security awareness training programme in place?
- ❑ Does the board receive frequent and regular updates on evolving threats?
- ❑ Is an incident response plan in place? Is it tested?
- ❑ Are business continuity plans in place? Are they up to date and tested across all shifts?
- ❑ _____
- ❑ _____

Technology and Services

- ❑ Is management tracking the latest technologies for cybersecurity?
- ❑ _____
- ❑ _____

1) ISO = International Organization for Standardization; NIST = National Institute for Standards and Technology.

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**

Cybersecurity Cheat Sheet for the Chief Executive Officer

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

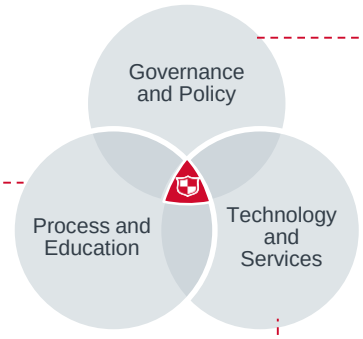
Amidst health care transformation, complicated federal regulation, margin pressures, and the push to innovate, adding the complex topic of cybersecurity to executive plates is understandably overwhelming. But the task of ensuring effective management of cyber risk falls to senior leadership. Examples 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 CEO Need to Be Involved in Cybersecurity Issues?

Cyber incidents can put an institution's ability to fulfil its mission to care for its patients and community at risk, so it is vital that CEOs ensure such risks are managed effectively. Beyond the potential for significant operational disruption, organisations face hefty costs and fines that easily stretch into the millions of dollars, and lasting reputational damage that may impact potential mergers, acquisitions, and partnerships. Additionally, CEOs and other C-suite executives may be held personally liable for the consequences of a cyber incident if they cannot demonstrate appropriate efforts at mitigation. CEOs have a responsibility to lead the institution in a positive security-focused culture, fostering an environment that engages all personnel and leadership. Key actions include demanding inclusive and thorough security governance and oversight; setting expectations for improvement in end-user training, testing, and preparedness; and not pointing fingers when an incident occurs. On the technology side, CEOs should focus not on understanding technical details of investments or specific ROI,[1] but on ensuring the organisation sees value from each.

1) ROI = Return on investment.

Critical Questions CEOs Should Ask About Cybersecurity

CEOs should proactively engage with both their board and leadership team on security issues and initiate a discussion with the board on security to establish their oversight role. Security must have a regular place on C-suite agendas. CEOs should ensure that all C-suite members have a clearly defined role and accountabilities for security matters. 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 CEOs 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

- ❑ Does the security governance structure engage all levels of leadership and enable staff to have a voice in decisions impacting their work?
- ❑ Is there a security strategy in place? Does it support the organisational strategy?
- ❑ Do you track progress according to a meaningful security dashboard that provides actionable information for making key decisions?
- ❑ To whom does the security officer report? Are they empowered with the authority required to make progress in the organisation's security posture?
- ❑ Who has the final say on risk assessments?
- ❑ Is there a continuous third-party risk management process in place?
- ❑ Do you include cybersecurity in due diligence of M&A[2] and partnership activities?
- ❑ _____

Process and Education

- ❑ Are executive-level security awareness training and testing in place? Are all executives included and required to take any necessary remediation training?
- ❑ Are robust security awareness training and frequent testing in place for all employees? Do you track testing results regularly? Do you see improvement over time? Are business leaders (not just IT) held responsible for improvement?
- ❑ Is there an incident response plan in place? Is it regularly tested? Are key personnel imbued with authority to make decisions in a time of crisis?
- ❑ What is your Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for your disaster recovery plans?
- ❑ _____

Technology and Services

- ❑ Are basic technologies such as encryption, mobile device management, and intrusion detection in place prior to investing in more complex security technologies?
- ❑ Do your security technology investments support the overall security strategy?
- ❑ _____

2) M&A = Mergers and acquisitions.

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**

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

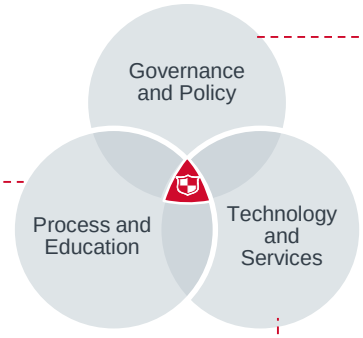
Amidst health care transformation, complicated federal regulation, margin pressures, and the push to innovate, adding the complex topic of cybersecurity to executive plates is understandably overwhelming. But the task of ensuring effective management of cyber risk falls to senior leadership. Examples 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?
- ❑ _____

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**

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.

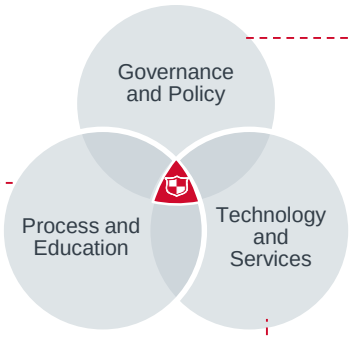
A Comprehensive Approach to Cybersecurity

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**

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.

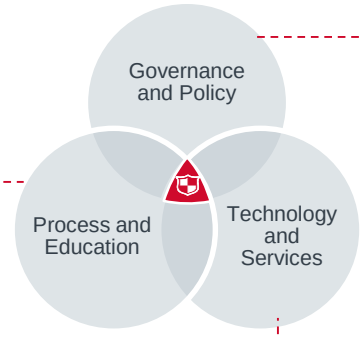
A Comprehensive Approach to Cybersecurity

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?
- ❑ _____

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**

Cybersecurity Cheat Sheet for the Chief Operating 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.

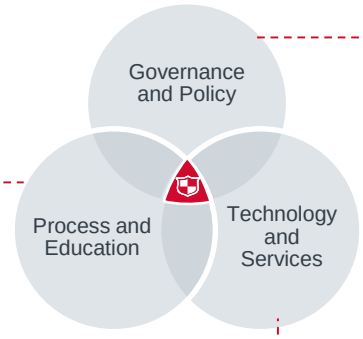
A Comprehensive Approach to Cybersecurity

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 COO Need to Be Involved in Cybersecurity Issues?

Effective cybersecurity preparations, especially business continuity planning and incident response planning, are critical to resilient processes that remain functional during and after cyber incidents. Disruptive attacks such as ransomware can take down essential business capabilities including email and telephone along with clinical systems. Incidents, whether a cyber attack or natural disaster, can strike at any moment without warning, so all staff (administrative and clinical) across all shifts (not just the overnight shift) must be trained and tested on the business continuity plan. Regular, frequent testing allows the COO and other key leaders to identify hiccups, adjust processes, and retrain staff as needed to ensure readiness. End users across the enterprise also must take immediate action if they notice suspicious activity or an attack on a workstation because a quick reaction can prevent larger, more widespread operational disruptions.

Critical Questions COOs Should Ask About Cybersecurity

COOs should proactively engage with 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, encourage robust and frequent security awareness training and testing, and ensure business continuity and incident response plans are in place, up to date, and tested frequently. 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 COOs 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

- ❑ Are adequate physical security policies and controls in place?
  - ❑ Do staff actually apply these policies in daily work (e.g., do they actually stop badge surfers)?
- ❑ How do you ensure end users have a voice in security governance for decisions that impact their daily work?
- ❑ Is a thorough security review included as part of any third-party vendor and non-employed partner relationship that operations may use?
  - ❑ Is there central visibility to track or know of all third parties in use?
  - ❑ Is the relationship, including access control, managed over time?
- ❑ _____

Process and Education

- ❑ Is frequent end-user training and testing in place? Is the organisation seeing improvement in testing failure rate over time? Do all staff require external email privileges?
- ❑ Are thorough business continuity plans in place? Are they up to date? Are they tested across all shifts? What are the sticking points that may require additional attention or retraining?
- ❑ How will you communicate to patients or the community should usual communication channels be down?
- ❑ How do you communicate to end users how certain security controls help protect the organisation and its patients?
- ❑ Do end users know immediate steps to take, including whom to notify when they first experience suspicious activity or an attack on their workstations?
  - ❑ Do users feel comfortable reporting incidents (i.e., do they feel they will not be blamed)?
- ❑ _____

Technology and Services

- ❑ How do the various technical capabilities impact end users?
- ❑ _____

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**

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.

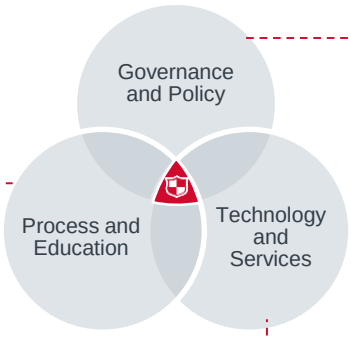
A Comprehensive Approach to Cybersecurity

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**

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.

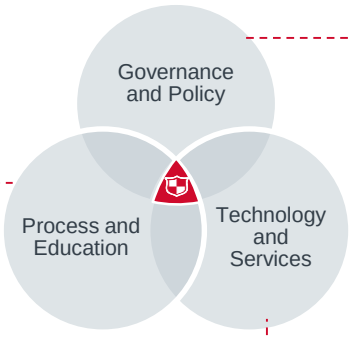
A Comprehensive Approach to Cybersecurity

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**