AAHC President's Council on Cybersecurity

Readiness | Response | Recovery

Cybersecurity at Academic Health Centers

Key Considerations for CEOs and C-Suite Leaders

Association of Academic Health Centers®
Leading institutions that serve society

aahcdc.org

READINESS

C-SUITE STRUCTURE AND GOVERNANCE

How cybersecurity is governed and managed across the academic health center to facilitate readiness

- Does the academic health center have a C-Suite structure that can respond to a cyberthreat? What is the chain of command for a cyberevent?
- Does the academic health center have a comprehensive team in place for cybersecurity (i.e., does the C-Suite team include leaders from legal, finance, and other areas in addition to IT)?
- Does the academic health center have adequate policies in place to prevent, respond to, and recover from a cyberevent?
- Are cybersecurity policies and strategies integrated and aligned across the academic health center (i.e., within institutions and across related institutions)? Do affiliation agreements or other documentation of relationships with partner institutions address issues of cybersecurity?
- How will institutional integrity be safeguarded in a cyberattack?
- How is your planned cyber response aligned with your overall business plan?

CYBERDRILLS

Use of simulated cyberevents to test strategies for responding to cyberthreats and understanding an academic health center's state of readiness

- When and how often are cyberdrills executed?
- Do the cyberdrills address the needs from the education, research, and patient care arms of the organization?
- How are lessons learned from cyberdrills reported and put into practice?
- Does the academic health center carry out its own testing of its systems to understand potential vulnerabilities?

CYBERINSURANCE

Insurance to cover damages from cyberevents

- Does the academic health center have appropriate insurance coverage for cyberevents?
- What is covered by current insurance policies in the event of loss from a cyberattack?
- What are the reporting requirements following a cyberevent to file a claim?

ENTERPRISE AWARENESS OF CYBER RISK

Ongoing awareness of the status of the academic health center's cybersystems

- Can the C-Suite team define the academic health center's threat surface?
- What mechanisms are in place to ensure 24/7 enterprise-wide awareness of cybersecurity health (e.g., dashboards, alert services)?
- At what point should the CEO and others in the C-Suite be notified of particular risks?
- How much capacity does the academic health center have to function without computer or internet access?
- Does the academic health center participate in proactive threat-hunting?
- Has the institution identified appropriate third-party cyberincident response groups?

CYBERSECURITY CULTURE

The culture of cybersecurity across the academic health center

- How are efforts to ensure cybersecurity embedded in the workflow and culture of the academic health center?
- Are academic health center community members aware of their responsibilities to ensure cybersecurity at the academic health center?

COMMUNICATION

Communication planning for cybersecurity and related events, including both internal and external responses

- Should there be a cyberevent, how will the academic health center communicate with its leadership, its internal community, third-party vendors, and the public?
- In the event of a cyberattack, how will the academic health center handle the surge of communication activity?
- How does the communication strategy utilize traditional and social media?

REGULATIONS

Funder and governmental regulations related to cybersecurity

- Should a cyberevent occur, what are the reporting requirements of academic health center regulators?
- How are cybersecurity regulations balanced with the academic health center's need for practical and innovative technology use to meets its mission?

LAW ENFORCEMENT

Awareness of local and national law enforcement assistance in preventing and recovering from a cyberevent

- During a cyberattack, when is it appropriate for academic health center officials to contact local and national law enforcement?
- What are the points of contact with local and national law enforcement during a cyberevent?

RESPONSE

C-SUITE ACTION

Considerations for C-Suite function during a cyberevent

- What is the full scope of the cyberevent in relation to impacted populations (e.g., patients, students, researchers) and assets (e.g., networks, hardware, systems, files)?
- How will the C-Suite team confirm the full scope of the cyberevent?
- Based on the nature of the cyberevent, what are the top-level objectives for responding and what are those objectives that can be triaged as secondary concerns?
- Have necessary resources (e.g., extra personnel, access to funds, decision-making authority) been made readily available?
- Has a briefing schedule been established for essential members of the C-Suite team to ensure that they remain current on the evolving nature of the cyberevent and their corresponding roles?
- What steps are being taken to protect the institutional integrity of the academic health center?
- Has the C-Suite team developed a plan to transition to normal operations?

COMMUNICATION

Communication with internal and external stakeholders, including the public, during a cyberevent

- How is the academic health center communicating the cyberevent to its internal and external stakeholders (e.g., via social media, the press, email)?
- Is it necessary to reach out to third-party cyberincident response groups?
- How is third-party communication (e.g., via the media, on social media) being monitored and responded to, if warranted?

CYBERINSURANCE

Insurance to cover damages from cyberevents

- Has the appropriate person contacted the appropriate insurance companies to report the event?
- How is the academic health center covered for the type of cyberevent being experienced?
- Are the necessary steps being taken to ensure the academic health center's ability to meet reporting requirements for filing a claim (e.g., preservation of evidence, documenting relevant events)?

RECOVERY

C-SUITE ACTION

How the C-Suite functions across the academic health center to recover from a cyberevent

- Has the CEO appointed a team to document the events of the cyberattack, its response, and lessons learned to provide feedback for future readiness?
- Which existing C-Suite policies and procedures worked well and which were suboptimal for readiness and response to the cyberevent?
- What was the overall impact of the cyberevent (e.g., financial loss, damage to reputation, regulatory penalties) and how will the C-Suite act to amortize any negative implications over time?
- Are additional efforts needed to address institutional integrity of the academic health center?

COMMUNICATION

Communication with internal and external stakeholders, including the public, about the impact of the cyberevent

- Based on an analysis of the experience, what improvements in communication should be implemented to enable the academic health center to provide even more timely and relevant information to its stakeholders about the nature of the cyberevent, the academic health center's response, and recovery efforts?

CYBERSECURITY CULTURE

The culture of cybersecurity across the academic health center

- How will efforts to safeguard against the root cause of the cyberevent be embedded in the workflow and culture of the academic health center?
- How does the academic health center balance security measures with maintaining workflow efficiency?

CYBERINSURANCE

Insurance to cover damages from cyberevents

- Did the academic health center's cyberinsurance policy meet the academic health center's coverage needs?

COUNCIL MEMBERS

EX OFFICIO

Released January 2020