Action Plan 2 for Governance and Leadership Support

By following this action plan and checklist, higher education institutions can ensure strong governance and leadership support for cybersecurity initiatives, leading to effective implementation of cybersecurity measures and protection against cyber threats.

1. Identify Key Stakeholders: Identify key stakeholders, including senior leadership, the Board of Trustees, and executive management, who will play a crucial role in supporting and championing cybersecurity initiatives.
2. Educate and Raise Awareness: Conduct cybersecurity awareness sessions and presentations for senior leadership to highlight the importance of cybersecurity as a strategic priority. Demonstrate the potential risks and implications of cyber threats on the institution's reputation, operations, and finances.
3. Align with Organisational Goals: Emphasise how cybersecurity aligns with the institution's overall strategic goals and objectives. Showcase how a robust cybersecurity framework enhances the institution's ability to achieve its mission and objectives.
4. Create a Cybersecurity Committee: Establish a dedicated cybersecurity committee with representation from senior leadership and relevant departments to oversee and guide cybersecurity efforts. This committee will be responsible for decision-making, policy approvals, and resource allocation.
5. Develop a Cybersecurity Strategy: Work with the cybersecurity committee to develop a comprehensive cybersecurity strategy that outlines the institution's vision, goals, and roadmap for enhancing security measures.
6. Budget Allocation: Secure adequate resources and budget allocation for cybersecurity initiatives. Present a business case that justifies the investment in cybersecurity and highlights the potential return on investment in terms of risk reduction and operational resilience.
7. Risk Communication: Ensure that senior leadership is regularly updated on the cybersecurity risk landscape and potential threats. Provide clear and concise risk reports and threat briefings to aid decision-making.
8. Council Engagement: Engage with the Council to gain their endorsement and support for cybersecurity efforts. Present the cybersecurity strategy and its alignment with the institution's overall strategic plan during board meetings.
9. Regular Reporting: Provide regular progress reports to senior leadership and the Board on the implementation and effectiveness of cybersecurity initiatives. Highlight key achievements, challenges, and areas for improvement.
10. Integration with Governance Structures: Integrate cybersecurity considerations into existing governance structures, such as strategic planning, risk management, and compliance.
11. Crisis Management Preparedness: Collaborate with senior leadership to develop a robust crisis management plan for cybersecurity incidents. Ensure that senior leadership is aware of their roles and responsibilities during a cybersecurity crisis.
12. Encourage a Culture of Security: Promote a culture of security from the top-down, emphasising that cybersecurity is a shared responsibility across all levels of the institution.

Action Plan 2 Checklist

✅ Identified key stakeholders, including senior leadership and the Board of Trustees.

✅ Conducted cybersecurity awareness sessions for senior leadership.

✅ Aligned cybersecurity efforts with the institution's strategic goals.

✅ Established a dedicated cybersecurity committee.

✅ Developed a comprehensive cybersecurity strategy.

✅ Secured adequate resources and budget for cybersecurity initiatives.

✅ Provided regular risk communication to senior leadership.

✅ Engaged with the Board of Trustees and gained their endorsement.

✅ Provided regular progress reports on cybersecurity initiatives.

✅ Integrated cybersecurity into existing governance structures.

✅ Developed a crisis management plan for cybersecurity incidents.

✅ Promoted a culture of security across the institution.