Action Plan 8 for Collaboration and Information Sharing

By following this action plan and checklist, higher education institutions can foster collaboration with other educational institutions and cybersecurity organisations, enhance information-sharing efforts, and collectively strengthen their cybersecurity posture. Collaboration and information sharing are key factors in building a resilient cybersecurity ecosystem within the education sector.

1. Establish Collaboration Partnerships: Identify and establish collaborative partnerships with other educational institutions, cybersecurity organisations, industry peers, and government agencies. Engage in regional and national cybersecurity networks and forums.
2. Share Best Practices: Actively participate in information-sharing initiatives to exchange best practices, lessons learned, and successful cybersecurity strategies with peer institutions. Share knowledge and experiences to strengthen collective security.
3. Threat Intelligence Sharing: Encourage and participate in the sharing of threat intelligence among educational institutions and cybersecurity organisations. Collaborate on identifying and mitigating emerging threats.
4. Participate in Cybersecurity Exercises: Engage in cybersecurity exercises and drills, such as tabletop exercises and red teaming, to test incident response capabilities and identify areas for improvement.
5. Collaborative Workshops and Seminars: Organise or participate in collaborative workshops, seminars, and conferences focused on cybersecurity. Use these opportunities to learn from experts, share experiences, and build relationships with other institutions.
6. Data Anonymisation: When sharing sensitive information, ensure that personally identifiable information (PII) is properly anonymised or removed to protect individual privacy.
7. Cybersecurity Task Forces: Join regional or national cybersecurity task forces that focus on specific threats or challenges faced by educational institutions. Collaborate on addressing common issues and sharing threat intelligence.
8. Participate in Information-Sharing Platforms: Engage in online platforms and mailing lists specifically designed for cybersecurity information sharing among educational institutions and relevant stakeholders.
9. Engage in Research Collaborations: Partner with other institutions in joint cybersecurity research projects to gain insights into emerging threats and innovative security solutions.
10. Create a Community of Trust: Foster a community of trust among collaborating institutions, where open and transparent discussions about cybersecurity challenges and incidents are encouraged.
11. Encourage Reporting: Encourage and support the reporting of cybersecurity incidents to relevant cybersecurity organisations or law enforcement agencies for broader threat awareness.
12. Regular Meetings and Updates: Schedule regular meetings with collaborative partners to discuss ongoing cybersecurity initiatives, share updates, and plan future collaborative activities.
13. Document Sharing: Share relevant cybersecurity documentation, such as incident response playbooks, policies, and procedures, with collaborative partners, and request access to their resources in return.
14. Support Regional Initiatives: Support and contribute to regional or national initiatives that aim to improve cybersecurity awareness and resilience in the education sector.

Action Plan 8 Checklist

✅ Identified and established collaborative partnerships.

✅ Actively participated in information-sharing initiatives.

✅ Engaged in threat intelligence sharing.

✅ Participated in cybersecurity exercises and drills.

✅ Organised or participated in collaborative workshops and seminars.

✅ Ensured data anonymisation when sharing sensitive information.

✅ Joined cybersecurity task forces or working groups.

✅ Engaged in online information-sharing platforms.

✅ Partnered in joint cybersecurity research projects.

✅ Fostered a community of trust among collaborative partners.

✅ Encouraged and supported incident reporting.

✅ Held regular meetings with collaborative partners.

✅ Shared relevant cybersecurity documentation with partners.

✅ Supported regional or national cybersecurity initiatives.