Action Plan 9 for Third-Party Risk Management

By following this action plan and checklist, higher education institutions can effectively assess and manage the cybersecurity risks posed by third-party vendors and service providers. This ensures that the institution's security is not compromised by potential weaknesses in the supply chain and helps maintain a strong overall cybersecurity posture.

1. Identify Third-Party Vendors: Create an inventory of all third-party vendors and service providers that have access to the institution's systems, data, or provide critical services.
2. Risk Assessment: Conduct a thorough risk assessment of each third-party vendor to evaluate their cybersecurity practices, data handling policies, and potential risks they pose to the institution's security.
3. Cybersecurity Standards and Practices: Establish a set of cybersecurity standards and practices that third-party vendors must adhere to. Include requirements for data protection, incident reporting, access controls, and vulnerability management.
4. Vendor Due Diligence: Conduct due diligence on potential vendors before entering into agreements. Review their cybersecurity policies, practices, and incident response capabilities.
5. Contractual Obligations: Include specific cybersecurity requirements in contracts and service level agreements (SLAs) with third-party vendors. Clearly outline the responsibilities of vendors for maintaining cybersecurity.
6. Continuous Monitoring: Implement a continuous monitoring process to assess the cybersecurity posture of third-party vendors regularly. Use security questionnaires, audits, and vulnerability assessments as part of the monitoring process.
7. Incident Reporting and Response: Require third-party vendors to promptly report any cybersecurity incidents that may affect the institution's data or services. Define the procedures for incident response and coordination.
8. Supply Chain Resilience: Assess the supply chain resilience of critical third-party vendors. Ensure they have robust continuity and disaster recovery plans to minimise disruption to services.
9. Vendor Security Training: Encourage third-party vendors to provide cybersecurity training for their employees to ensure they understand and follow the institution's security policies.
10. Security Assessments for Changes: Conduct security assessments when significant changes occur within the third-party vendor's organisation, such as mergers, acquisitions, or changes in management.
11. Security Review Meetings: Conduct regular security review meetings with key third-party vendors to discuss cybersecurity concerns, share best practices, and address any emerging risks.
12. Exit Strategy: Develop an exit strategy to manage the transition away from a third-party vendor if they fail to meet cybersecurity standards or if the vendor relationship is terminated.
13. Contract Renewals: Review cybersecurity standards during contract renewal discussions to ensure they are up-to-date and align with the institution's evolving security needs.
14. Escalation Process: Establish an escalation process to address significant cybersecurity concerns with third-party vendors at the executive level if necessary.

Action Plan 9 Checklist

✅ Created an inventory of third-party vendors.

✅ Conducted a thorough risk assessment of each vendor.

✅ Established cybersecurity standards and practices for vendors.

✅ Conducted due diligence on potential vendors.

✅ Included cybersecurity requirements in vendor contracts.

✅ Implemented continuous monitoring of vendor cybersecurity.

✅ Required incident reporting and response from vendors.

✅ Assessed supply chain resilience of critical vendors.

✅ Encouraged vendor security training for their employees.

✅ Conducted security assessments for significant changes.

✅ Held regular security review meetings with vendors.

✅ Developed an exit strategy for vendor relationships.

✅ Reviewed cybersecurity standards during contract renewals.

✅ Established an escalation process for significant concerns.