VENDOR CYBERSECURITY CHECKLIST

Vetting Your Vendor's Cybersecurity Management

It's essential to ask the right cybersecurity questions and obtain the correct documentation to fully understand the residual risk from outsourcing a product or service to a vendor.

This vendor cybersecurity checklist can help. Be sure to retrieve information surrounding the following:

Security Testing

Vulnerability Testing (Periodic or Ongoing)

- Were any critical or high-risk vulnerabilities found?
- Were those vulnerabilities mitigated or remediated?
- Does the vendor have a plan in place to prevent similar vulnerabilities in the future?

Penetration Testing (Application, Internal/External Network)

- Are penetration tests performed by a qualified third-party vendor? If so, how often are they performed and when was the last test performed?
- Were any critical or high-risk vulnerabilities found?
- Were those vulnerabilities mitigated or remediated?
- Does the vendor have a plan in place to prevent similar vulnerabilities in the future?

Social Engineering (Phishing and Vishing Training and Testing)

- Were any critical or high-risk vulnerabilities found?
- Were those vulnerabilities mitigated or remediated?
- Does the vendor have a plan in place to prevent similar vulnerabilities in the future?

Remember: Ensuring your technology vendor performs regularly scheduled security testing is essential in knowing how secure their environment is and where the weaknesses are so they can be secured before they're exploited by an attacker.

Data Security

Encryption Standards

- What encryption algorithms are used for data in transit and at rest?
- How is data protected in transit between the vendor and the client as well as between the vendor and the end-user?

Data Retention/Destruction Policies

- How is data protected on servers and backup media?
- Is there evidence of a documented policy which outlines practices for data destruction?
- Does the vendor perform physical document destruction, such as paper shredding and disposal?
- Does the plan include electronic media sanitization, erasure, wiping, degaussing or destruction?

Data Classification and Privacy Policy

- Is there a formal information security program in place? If so, does it include how data throughout the organization is classified and subsequently protected?
- Is a privacy policy in place to explain how sensitive data is used, disclosed, protected and ultimately destroyed?

Remember: A security program provides the framework for keeping an organization at a desired security level by assessing the risks that are faced, deciding how those risks will be mitigated and planning for how to keep the program and security practices current.

Having a comprehensive vendor cybersecurity checklist can create process efficiencies and help prevent risk exposure.

SAVE CHECKLIST **PRINT** CHECKLIST

Incident Detection and Response

Documented Incident Response Plan
- Does the incident management plan include detailed provisions around preparation, identification, containment, eradication, recovery and lessons learned?
- Does the plan specify how to respond to different types of incidents such as phishing attacks, ransomware attacks, malware, viruses, etc.?

Notification Process/Timeliness
- Are the appropriate and satisfactory notification stipulations clearly mapped out in the incident response plan?
- Does the plan specify the role of the information security team within the notification process?

Incident Detection Controls
- Are incident detection tools such as intrusion detection and prevention tools, firewalls, anti-malware products, as well as patch management practices in place and functioning?

Cybersecurity Insurance Policies
- Does the vendor have cybersecurity insurance coverage?

Remember: Proper incident handling procedures allow situations to be analyzed and prioritized so that the next appropriate course of action can be taken to address the problem. Breach notification, a key component of incident management, is now included within multiple regulations with emphasis on vendor reporting.

Employee, Contractor and Vendor Management

Hiring Background Checks
- Does the vendor perform rigorous pre-employment screening?
- What due diligence is performed on contractors and vendors prior to and post contract?

Annual Privacy and Security Training
- Are employees and contractors required to complete security awareness training?

Access Management Policies
- What are the details of the vendor's termination procedures?
- Has the vendor implemented the principles of least privilege and segregation of duties?
- Is there a formal logical access review process?

Confidentiality & Non-Disclosure Agreements (Contractors, Employees, Vendors)
- Are there confidentiality and non-disclosure agreements in place where they should be?

Remember: Role-based access privileges are vital in allowing employees to have access to only the data they need to perform their job functions. Having regularly scheduled access reviews of users is essential in knowing who should and shouldn't have access to a system. Failures in logical access review procedures are the top reason for exceptions in SOC reports.

Pro Tip: Ensure your vendor's vendor risk management program supports this level of detail and that it's okay to ask for evidence of this review, redacted if necessary, for any fourth party that plays a key role in providing contracted services or that also has access to your data.