Critical Questions to Evaluate the Security Trustworthiness of an MSP

GIBRALTAR®
DRIVING DIGITAL TRANSFORMATION

MSPs play a vital role in ensuring the security and functionality of your digital estate. However, not all MSPs are created equal, and some may fall short of delivering the trust and security your business demands. Here are vital questions to help you determine if you can trust the MSP's security capabilities:

Data Protection and Privacy

- [ ] How do you safeguard sensitive customer and business data from unauthorized access?
- [ ] Can you explain the methods you employ to protect data at rest and in transit?
- [ ] Are you compliant with relevant data protection regulations? (e.g., GDPR, HIPAA)?
- [ ] How long do you retain customer and business data, and what is your process for securely disposing of data that is no longer needed?

Access Controls

- [ ] How do you manage user access to systems and sensitive data?
- [ ] Are there different levels of access privileges for different users within your systems, and how are these roles assigned and managed?
- [ ] What methods do you use to authenticate users before granting access?
- [ ] Do you have a process for regularly reviewing and managing privileged access?
- [ ] How do you monitor user activity and access logs?
- [ ] Can you explain your process for auditing access and detecting unusual or unauthorized activity?

Incident Response

- [ ] What is your approach to handling security incidents and breaches?
- [ ] What is your typical response time to different levels of incidents?
- [ ] What are your protocols for notifying affected parties in case of a data breach?
- [ ] How frequently is the incident response plan reviewed and updated to address emerging threats?
- [ ] Can you provide an example of a recent incident you successfully mitigated?

Vulnerability Management

- [ ] What tools and methods do you use to identify vulnerabilities?
- [ ] What steps do you take to remediate vulnerabilities once they are identified?
- [ ] How do you prioritize and apply security patches to mitigate vulnerabilities?
- [ ] Can you explain your process for testing and deploying patches while minimizing system downtime?

Security Audits and Assessments

- [ ] What frameworks, standards, or best practices do you follow for assessments?
- [ ] What systems, processes, and assets are typically included in your assessment?
- [ ] How often do you conduct security audits and assessments?
- [ ] How do you present findings and recommendations to clients for improvement?

Disaster Recovery and Business Continuity

- [ ] Can you provide an overview of your disaster recovery plans and strategies?
- [ ] How frequently do you back up our data, and what methods do you use for backups?
- [ ] Can you describe your data restoration processes in the event of data loss?
- [ ] How often do you test your disaster recovery and business continuity plans?
- [ ] How do you prioritize which systems and applications are critical for business continuity?

Third-Party Risk Management

- [ ] How do you evaluate the security practices of third-party vendors you may work with?
- [ ] What steps do you take before onboarding a new third-party vendor?
- [ ] How do you continuously monitor the security practices of third-party vendors?
- [ ] What measures do you have in place if a vendor's security practices do not meet our expectations?

Compliance and Certifications

- [ ] What industry-specific certifications do you hold that are relevant to our business and security requirements?
- [ ] How do you ensure compliance with relevant security regulations?
- [ ] Do you maintain documentation of your compliance efforts and certification status?
- [ ] How do you stay informed about changes to relevant regulations and standards that might impact our security posture?

Transparency and Reporting

- [ ] How do you inform us about security incidents, vulnerabilities, and remediation efforts?
- [ ] Do you provide regular security reports detailing your activities and findings?
- [ ] Are clients able to request additional information, logs, or documentation related to security events and activities?

Employee Training

- [ ] How do you ensure that your staff is well-trained in cybersecurity best practices?
- [ ] Can you provide an overview of the training programs you have in place?
- [ ] How often do you conduct security training sessions for your employees?
- [ ] How do you assess the effectiveness of your security training programs?

References and Case Studies

- [ ] Can you provide references from clients who have faced security challenges and benefited from your services?
- [ ] Do you have any case studies highlighting your success in enhancing security for other businesses?

Prepare and Protect Your Digital Estate with Gibraltar

Gibraltar Solutions provides leading IT security knowledge, tools, services and employee training to protect your organization today and in the future.