CompTIA

A CEO's Guide to Choosing an IT Service Provider

Cybersecurity questions for business leaders to ask potential MSP partners

Table of Contents

Overview

The decision to select an IT service provider or managed service provider (MSP) is critical to any organization. As a business or technology leader, you need to be prepared to ask the tough, important questions to ensure that your IT provider is qualified to meet your needs. Along with legal and accounting, there are few service categories that require a trusted partner to handle and manage sensitive information as your technology provider. Choosing an IT partner requires someone who can be trusted to design, access, administer and secure your computer networks and data.

The CompTIA Cybersecurity Advisory Council developed this guide to help you ask the right questions—and solicit the right answers—regarding the support, stability, and security related to your systems. In addition, it will help you get clarity around how a service provider treats its own systems where your sensitive information may be stored and how remote access will occur. An IT service provider's weak security practices could result in a cyber incident that in turn compromises its clients' information too.

Below are recommended questions to consider asking your IT service provider or MSP. The questions should serve as a guideline but can be adjusted to fit your specific needs and complexity. Use this guide as a pre-selection tool to help select a new IT provider, or to help evaluate the partner that you already leverage for technology support.

Have your IT provider fill out this form or answer these questions to get the insights needed to help choose the right partner for your company.

Company Background – Pre-Sales

These are pre-relationship questions a business should ask a prospective information technology service provider. The goal is to help you determine if they are qualified.

1. Do you operate your firm with at least the same level of security as you recommend to your clients? If no, please explain in detail why not and what is different.

2. Do you have qualified security resources who are specifically assigned to keeping your network safe? If no, please explain in detail.

3. If you do not have inhouse security experts, do you leverage the expertise of qualified security professionals outside your organization that are responsible for the security and assessment of your systems? If no, please explain in detail why not and what compensating controls / solutions are in place:

4. Have your systems, policies and procedures been independently assessed by independent, qualified professionals outside your organization for security effectiveness and enforcement? If no, please explain in detail what validation processes are used to ensure the above.

5. Has your firm had any core services or systems outages that impacted your ability to operate, support clients' systems or client services in the last 12 months? If yes, please explain.

6. Has your firm had any significant network (or other system) security incidents in the last 36 months? If yes, please explain.

7. Has your firm ever had a cyber incident determined to be reportable to law enforcement or federal or state regulatory bodies? If yes, please explain.

8. Have you ever made a claim against your cyber liability or breach coverage? If yes, please explain.

9. Is your firm, or has your firm or any organization it relies upon for client services, ever filed for bankruptcy or receivership?

10. Is your firm currently subject to any civil or criminal investigation? If yes, please explain.

11. Do you subcontract your infrastructure or the services you provide to clients?

If yes:

a. For what areas?

b. How are these subcontractors vetted?

c. How are they monitored while working within or at your client's environment?

d. Do you require subcontractors to have similar terms and conditions in your mutual agreements as those signed with your clients?

e. What kinds of agreements are contractors required to sign when providing services for you or your clients?

f. Are employees and contractors limited to minimum access necessary to systems and information?

MORE ADVANCED VETTING

1. Do you run criminal and other personal and professional integrity checks on employees before they are hired?

2. Within legal constraints of what is allowed, do you limit who may be hired based on criminal history?

3. Do you drug test employees for illicit drug use before hiring and/or randomly?

4. Do you verify references for all employees and vendors?

5. Do you require attestation of compliance with agreements and cyber hygiene?

6. Do you contact comparable references?

TRAINING

1. Do you provide cyber security technical and social awareness training to your employees?

   a. How often? _____

   b. Are they tested? _____

      i. How? _____

Frameworks/Compliance

These questions are designed to ensure your provider can meet your data security and regulatory obligations and that they are compliant themselves.

1. Do you manage your systems following a cybersecurity framework? If the answer is yes, which framework?

2. Do you document your compliance?

3. Is your compliance audited?

4. Are your systems audited for compliance with policies?

5. Can you support governance requirements or cyber insurance obligations?

Policies

These questions are designed to ensure that your IT provider has documented processes and appropriate policies.

1. Please describe your change management process.

2. What is your documentation policy about ensuring that we have all of the documentation we need to operate without your involvement?

3. Please list and describe (by name only) what policies you have in around use, privacy, and data retention, etc.

4. Do you have a well-defined employee and vendor sanction policy that guides your response to policy violations?

5. Do you have a privacy policy that relates specifically to the creation, use and destruction of client data?

Privilege Account Management

These questions are designed to ensure that your IT provider understands appropriate access policies.

GENERAL

1. Please described privileged access to clients' systems.
   a. How is access assigned? _____

   b. How is it limited? _____

   c. How is it monitored? _____

   d. Are controls in place to limit access to the needs of their roles? _____

2. Are users restricted to non-admin accounts for anything that does not require admin rights?

   _____

   _____

3. Are privileged and/or admin or other management level accounts shared and if yes:
   a. Why? _____

   b. Which accounts? _____

   c. What are the mitigating controls? _____

   d. How do you ensure accountability? _____

4. What tools and access methods are used for network administration and client support functions?

   _____

   _____

5. Do you have account creation or rights level change alerts configured?

   _____

   _____

ROLE-BASED ACCESS CONTROL (RBAC)

1. Are you enforcing least privilege for all systems?

2. How do you manage additions, moves and changes of users and their rights?

3. Do you require different credentials for every client?

4. How are credentials changed when employees who may have had access leave your firm?

5. How often do you review user rights to insure against access creep?

AUTHENTICATION MANAGEMENT

1. Are you using multifactor authentication for all network access and privileged/admin functions?

2. Do you validate the identity of individuals inquiring about client systems and/or/ requesting support?

PASSWORD MANAGEMENT

1. Are you using complex passwords with at least 12-characters?
2. How often are password changes required?
3. Do you use password library and past password validations?
4. Do you require that no passwords for any user be set to never expire?
5. How often are privileged/admin or other management accounts' passwords changed?

SESSION MANAGEMENT

1. Do you use account lockout functions for failed access attempts?
   a. How many attempts?
   b. How long?
   c. What is the reset function?
   d. How is this process audited for potential nefarious activity?
2. Do you have idle account lockout configured?
   a. If yes, how long before lockout?

Systems Management

These questions are designed for you to have a general understanding of your IT service provider's internal controls.

1. Do you have a Bring Your Own Device policy? _____
   a. How is company/client data managed on these devices?
   _____
   b. Do you have a compliance program for BYOD? _____
2. Are the devices under management by you and being used to support clients' systems or storing clients' data in a private and contained area that is restricted access?
   _____
3. Are any of your clients' assets in comingled multi-tenant architecture within your environment or shared environments contracted for by you?
   _____
4. Do you maintain accurate as built documentation for your network infrastructure?
   _____
5. Are you operating with any unsupported hardware of software? _____
   a. If yes: please explain.
   _____
   b. What controls are in place to manage the increased risk?
   _____
6. Do you allow Wi-Fi access to corporate assets? _____
   If yes, please describe the security measures used to protect critical corporate assets that could impact operations, enable threat actors to gain a foothold or otherwise impact clients.
   _____
7. Can you quickly identify new devices attached to your network?
   _____
8. Do you have physical and digital controls to disallow the attaching of unapproved devices?
   _____
9. What physical measures are in place to protect your devices?
   _____
10. Are all physical and systems' access events individually identifiable and auditable?
    _____

Incident Response

These questions are designed to determine if your IT service provider has a documented plan in preparation for a cyber or other incident.

1. Do you have documented incident response plans?

   a. How often are they updated?

   b. How often are they tested?

   c. Have you had any significant incidents in the past 12 months?

      i. Please explain

2. If you were to be hit by a ransomware attack, please describe (on a high level) the recovery process you would follow and how the attack could impact customers?

   a. What are the recovery time objectives?

   b. What is the continuity plan?

3. If you suffered a general cybersecurity incident, do you have clearly defined and documented response steps in written form, not stored on your potentially impacted corporate assets?

4. Who owns the responsibility for the plan, response and is there a succession plan?

5. Do you have a qualified crisis manager?

Critical Patch and Vulnerability Management

These questions are designed to ensure your service provider maintains patch and vulnerability management for themselves and for customers.

1. Do you have a documented vulnerability management program?

2. Do you conduct regular vulnerability assessments of your systems and how often?

3. What is the remediation time expected for vulnerabilities identified in your environment?

   a. Critical

   b. High

4. Systems patching against critical vulnerability:
   a. Please describe your device firmware and software updating process.

   b. How often are patches applied and how are patches selected and vetted?

   c. What is the normal security patch schedule for desktops and servers used to support clients' services and store clients' information?

   d. What kind of maintenance notices are provided when downtime may be required?

   e. Do you require system restart as needed (post patch application)?

   f. Do you do post patch validation and smoke testing to ensure functionality and patch application was successful?

Detection / Prevention

These questions are designed to ensure continuous monitoring, detecting and responding to events.

1. Do you have an MDR, SIEM and/or other solutions monitoring your infrastructure and or shared infrastructure being used to support client services? Please explain in detail.

2. Log management:
   a. Please describe your log capture, storage and retention process.

   b. Are logs stored offsite and protected from threat actors?

   c. Please describe your log collection and verification process.

   d. Please describe access replay functionality.

   e. Are there insider protections in place against the deletion or modification of logs?

3. Do you require logon banners declaring that the systems contain confidential and proprietary information, and warning of employment action and potential criminal prosecution for any unauthorized access or use of the systems?

4. Are all devices (servers, desktops, laptops, phones, portable USB/Flash drives, etc.) that contain client data encrypted?

   a. If yes, using what encryption mechanisms, key management, access rules and policies?

   b. If no, what compensating controls are in place?

5. Do you block access to known malicious websites?

6. Are you using enterprise level, centrally managed end-point protection against malware?

7. Do you use DNS / URL reputation services?

Service Recovery

These questions are designed to ensure that your IT service provider are available when you need them.

BACKUPS

1. Are your internal and external backups encrypted? _____
2. If backups are encrypted, how are the keys managed?

   _____

   a. Who has access? _____

   b. How is access audited? _____
3. Do system redundancies, backup, or other functions result in client data potentially leaving the United States?

   _____
4. Are backups stored offsite and out of reach of threat actors?

   _____
5. Are backups protected by multifactor authentication and is there restricted access?

   _____
6. What specific insider protections do you have in place to protect systems from both employees and potential threat actors?

   _____

   a. Could a domain administrator delete, corrupt, disable or otherwise interfere with or damage your backups? _____

   b. Is there insider protection and integrity monitoring for backups? _____

RECOVERY PLANNING

1. Do you have a documented Business Continuity Plan? _____

   If yes:

   a. When was the last test? _____

   b. What was the result? _____
2. Do you have a documented Disaster Recovery Plan? _____

   a. If yes, when was the last test? _____

   b. What was the result? _____
3. What are the RPO and RTOs for your core services that support services we are receiving?

   _____

Security Assessments

These questions are designed to ensure that your organization identifies and hardens attack surfaces.

1. When was your last risk assessment performed and who completed this task?

   _____

   a. Were there critical findings? _____

   b. *If yes:*

      i. Were those findings remediated? _____

      ii. Were those remediations validated? _____

2. Do you regularly conduct internal and external penetration test? _____

   If yes:

   a. How often? _____

   b. What kind? _____

   c. When was the last test? _____

   d. Were all adverse findings remediated? _____

   e. Who conducts your internal and external vulnerability testing? _____

3. Is the penetration tester independent of your current IT team? _____

Insurance

These questions are designed to ensure that appropriate coverages are in place.

1. Do you carry general liability insurance? _____
    a. What coverages? _____
    b. How much? _____
    c. Are there sub limits or exclusions? _____
2. Do you carry errors and omissions insurance? _____
    a. What coverages? _____
    b. How much? _____
    c. Are there sub limits or exclusions? _____
3. Do you carry cyber breach and ransomware insurance? _____
    a. What coverages? _____
    b. How much? _____
    c. Are there sub limits? _____
    d. Are there any exclusions for ransomware? _____

About the Cybersecurity Advisory Council

The CompTIA Cybersecurity Advisory Council brings together thought leaders and innovators from a multitude of disciplines, working together to educate technology solution providers on the latest and greatest cybersecurity practices and protocols for business.

What We Stand For

Cybersecurity is a critical component for every business and any technology solution today, but one that requires constant vigilance, collaboration, and communication. We strive to address some of today's most pressing issues and threats, providing guidance for businesses of all sizes on how to find and work with the right technology service provider.

How We're Making an Impact

The pressure from hackers and other bad actors isn't abating. It's critical for all companies to establish effective and vigilant cybersecurity protocols as well as develop the next generation of resources that will be required to protect assets The Cybersecurity Advisory Council's roster of industry experts and thought leaders offers the guidance and tools necessary to help tech businesses stay ahead of the curve.