Questions to ask
a potential cybersecurity partner

LeapFrog®

One of the most effective ways to get security under control is to team up with the right outsourced IT partner.

A Managed Service Provider (MSP) or Managed Security Service Provider (MSSP) has security experts and processes in place and follows proven methodologies that protect and defend IT environments. They also have the capabilities to jump in to help their partners recover quickly if they do experience an attack.

But choosing the right IT partner isn't easy.

It's important to find an experienced, disciplined company you trust and want to work with for several years or longer. Whether you lead an IT department or are a CFO or CEO in charge of IT strategy, this guide will help you ask the right questions during your initial cybersecurity partner interviews.

Start with developing a potential partner shortlist. Ask people in your industry or trusted advisors for referrals and check out the referred websites, as you would during any discovery process. In particular, look for:

- Their approach to cybersecurity
- If they manage security or are a VAR that sells hardware or software
- Information that shows their proficiency in all areas of cybersecurity

The companies on your shortlist should want to talk with you. They should be interested in hearing about your security needs and concerns and discuss how their company can help address these issues for you.

Ask questions about:

- **Company Background**
- **Sustainability and Growth**
- **Cybersecurity Background**
- **Cybersecurity Delivery**
- **Risk and Expectations**

During the first meeting (usually a phone call), you'll be able to get a sense of their business model, company culture, and skills. You may need two meetings to cover all of the questions on the following five slides.

Company Background Questions

Question	Answer to look for
1. Can you talk to me about your business processes?	Proactive, consistent processes that drive performance and stability.
2. How is your company structured?	A clear overview of their teams and how they work, including the number of engineers on staff and the makeup and specialties of their escalations teams.
3. What is your toolset?	A recognizable set of industry security tools, including software and hardware solutions, that are suitable for servicing your existing environment. They should be able to discuss their toolset in depth and instill confidence that they have plenty of experience using it.
4. Which client platforms and technologies are you most comfortable with?	Include the technology brands you currently use in-house or want to use. Examples of platforms include Tenable, Cisco, Fortinet, and Secureworks, and examples of technologies include well-known brands of firewalls, switches, and servers.
5. Can you describe your typical clients for me — what size and how many?	Confirmation they have a lot of experience working with companies like yours.

Sustainability and Growth Questions

Question	Answer to look for
1. Generally speaking, what is your average client tenure?	They have been working with some clients since inception and have new clients, too — this means the company is stable and growing. The longer the average tenure, the better.
2. And how about your employees — what's the average tenure?	The same response as client tenure. A mix of both long-term employees and new hires is best.
3. Given the high levels of IT turnover and the tech-talent shortage, what's your process for staying fully staffed or quickly ramping up when you need to?	A strategic, solid process for locating, hiring, and onboarding quality tech staff in a relatively short amount of time. This allows for stability and follow-through.

Cybersecurity Background Questions

Question	Answer to look for
1. What kind of security expertise do you have?	An operational approach that integrates security at every level when managing IT. Security should not be a product or add-on feature.
2. Is your company SSAE 18 SOC 2 compliant?	Affirmation that they comply with auditing standards for service organizations. MSPs and MSSPs that follow best practices themselves are best positioned to help you do the same.
3. What are the most common types of cybersecurity issues your clients deal with?	The same types of issues you're concerned about. Examples include getting hacked, ransomware, fraud, unauthorized access, brand reputation, DDoS attacks, cyber warfare, data loss, and insider threats.
4. How do you usually handle those issues when they come up?	A commitment to follow ITIL (IT Infrastructure Library) practices. Ideally, they'll talk about a consistent methodology being the key to handling security issues whenever they come up, including how to handle mega-hacks.

Cybersecurity Delivery Questions

Question	Answer to look for
1. Talk to me about how you usually handle isolated, specific-client issues.	By following best practices. They should adhere to an incident management process, either ITIL or ISO (International Organization for Standardization).
2. How do you handle security issues when they're more system-wide or impact multiple clients simultaneously?	Again, by following ITIL or ISO best practices. They should adhere to major incident management and security incident response planning to ensure the fastest, most effective response, regardless of the breadth of the security issue.
3. What is your methodology to reassess our level of risk as we progress?	Processes that include constant re-evaluation and enhancements after having designed and deployed your improvements.
4. Who specifically have you worked with that has had problems like ours?	At least one or two recent success stories and preferably plenty of examples of institutional knowledge related to your specific problem areas.
5. What is your typical timetable for being able to improve security for your new clients?	A realistic approach — it's unlikely an experienced MSP or MSSP that follows best practices will be able to offer a quick-secure option.

Risk and Expectations Questions

Question	Answer to look for
1. Talk to me about the risk evaluation process you'll use to determine what you'll recommend for us?	An iterative process that includes weighing risk as part of an IT impact analysis for your business overall. The methodology should be based on what you told them and not a predetermined package.
2. What can you tell me about the kinds of results we can expect?	Confirmation that you can expect the same kinds of results that their other clients have experienced. They should be able to provide data that show marked improvements.
3. What improvements have you made to your own security processes since last year?	Have integrated new tools, roles, and compliance standards. They should also have made adjustments based on evolving cybersecurity threats.
4. What kind of transparency and reporting do you provide?	A portal or system that catalogs your company's business policies, procedures, compliance evidence if needed, and regular, meaningful reporting on the health of your security program. You should also be able to see active issues and what's being done to resolve them.

Ask Your Team: The Vetting Process

Your organization can feel confident moving forward by choosing an outsourced IT partner that enables you to put all of the critical cybersecurity pieces in place — people, processes, and tools.

People	Processes	Tools
Do they share our business principles and seem culturally and philosophically compatible?	Do they follow best practices, both internally and with their clients?	Is their toolset a good match for us?
Do they have the levels of experience, capabilities, and stability that we need?	Do they have an effective methodology to deliver on their security promises even when multiple clients need attention?	Will they follow our company's policies and provide transparency into the state of our security program and any issues we're experiencing?
Since we'll be interfacing with the company frequently, is there natural chemistry between our people?	Are they among the best of breed for cybersecurity?	Are we confident their team will stay on top of the most effective tools for emerging threats?

Choose peace of mind

Your chosen partner will provide something intangible along with proven methodologies to secure your IT operations. They give you peace of mind.

With consistent, reliable protection against external and internal attacks and other IT disasters, you can avoid disruptions to your business, respond and recover more quickly when problems do arise (no methodology is foolproof), and limit your potential financial loss. Teaming up with the right partner for the long term also helps protect your brand and attract new business.

Securing your IT operations is too important to ignore. It's time to develop your short list and start interviewing!

Leapfrog Services is an IT Security, Network, and Infrastructure Managed Service Provider (MSP/MSSP) that's been helping organizations meet their business goals and protect their data since 1998.

Our team designs and operates outsourced solutions based on our proven methodology that includes matching your level of threat protection to your business needs and adhering to the highest cybersecurity standards (we are SSAE 18, SOC 2, and PCI compliant). Guarding against risks systematically and consistently reduces the likelihood your organization will be attacked and helps you to remain productive and successful.

You can call us at 866-260-9478 or email us at sales@leapfrogservices.com.