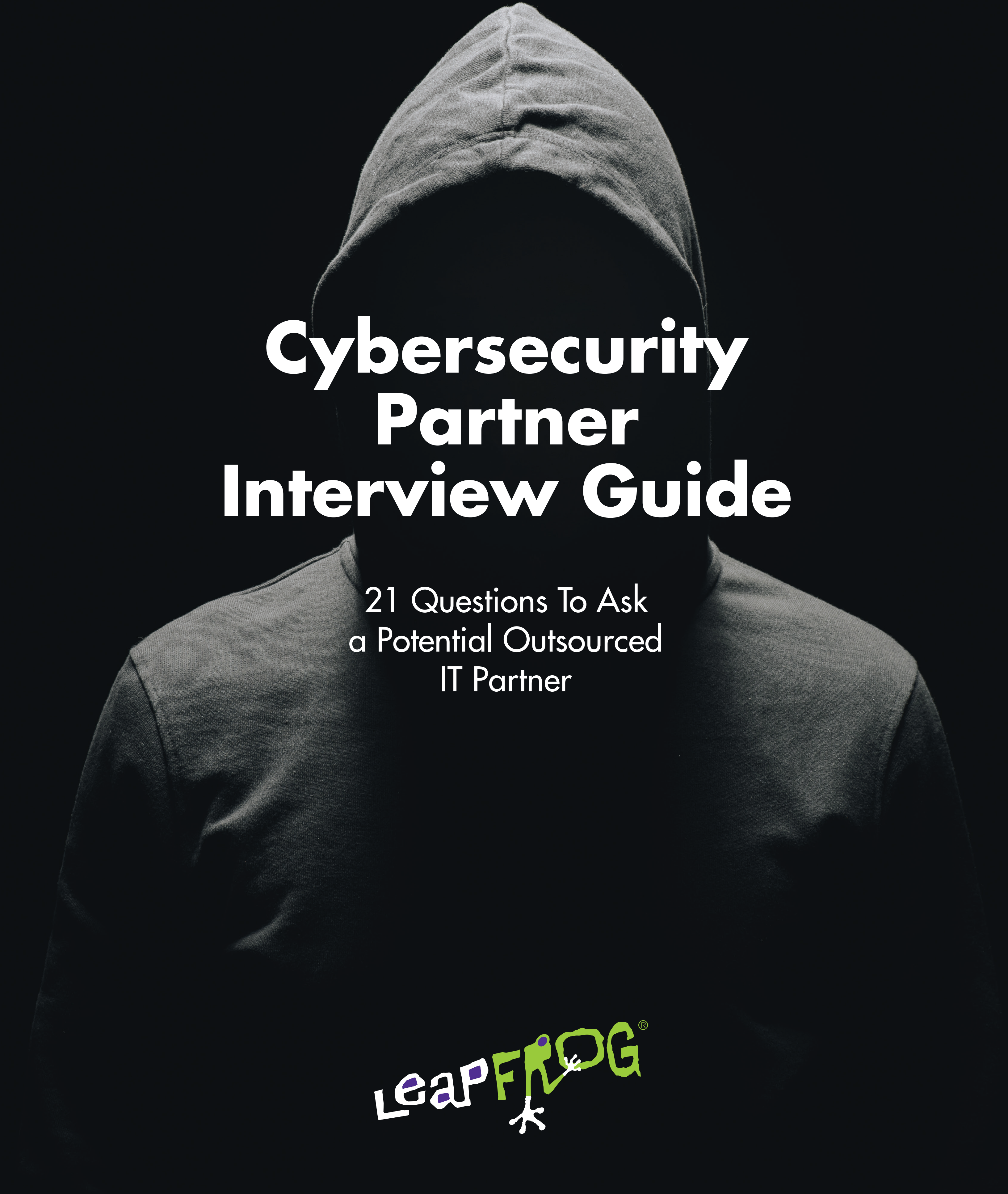
Leapfrog's TechBrief



Cybersecurity Partner Interview Guide

21 Questions To Ask a Potential Outsourced IT Partner

LeapFROG®

Cybersecurity Partner Interview Guide

With cybersecurity risks increasing — including mega-hacks like the SolarWinds and Microsoft Exchange Server hacks — organizations need to take action. One of the most effective ways to get security under control is to team up with the right outsourced IT partner.

Managed service providers (MSPs) have security experts and processes in place and follow 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’re an IT leader or CFO or CEO in charge of IT strategy, this guide will help you ask the right questions during your initial partner interviews.

“The type of corporate information cyber attackers have access to is pure gold: information on pricing structures, strategic bids, client lists – the possibilities are endless.”

– Mark Logsdon, The AXELOS Blog, Preventing cyber attacks - it's a people thing as much as IT

Step One:
Develop your potential partner shortlist

You should be able to learn high-level information by looking at their websites:

- What is their approach to cybersecurity?
- Are they an MSP that operates and maintains technology or a VAR (value-added reseller) that sells third-party hardware and software?
- Are they an established organization with a demonstrable track record?
- Do they provide information about cybersecurity, compliance, and disaster recovery?
- Does it appear they have the breadth and depth to fully support our organization?
- Is their leadership experienced enough to handle major events?
- Do they work with companies like ours?

Step Two:

Ask these 21 questions during your partner interviews

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. 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.

Company background questions

1. **Can you talk to me about your business processes?**

   Look for: Proactive, consistent processes that drive performance and stability.

2. **How is your company structured?**

   Look for: A clear overview of their teams and how they work, including how many engineers they have on staff and the makeup and specialties of their escalations teams.

3. **What is your toolset?**

   Look for: 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.

> "Buying malware is currently not a problem: it's easy to find them on various hacker forums, and they are relatively cheap, making them attractive. A cybercriminal following this illegal path doesn't even need any skills – for a fixed price they can get an off-the-peg package to launch their attacks at will."
> *– Alexander Gostev, Chief Security Expert at Kaspersky Lab*

4. **Which client platforms and technologies are you most comfortable with?**
   Look for: Technology brands that you're currently using in-house or that you 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 a typical client for me? What size companies do you usually work with and how many clients do you have?**
   Look for: Confirmation that the potential partner has a lot of experience working with companies like yours.

Stability and growth questions

6. **Generally speaking, what is your average client tenure?**
   Look for: Partners that 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.

7. **And how about your employees — what's the average tenure?**
   Look for: The same response as client tenure. A mix of both long-term employees and new hires is best.

8. **Given the high levels of IT turnover and the growing tech-talent shortage, what's your process for staying fully staffed or quickly ramping up when you need to?**
   Look for: 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.

General cybersecurity questions

9. What kind of security expertise do you have?

Look for: An operational approach that integrates security at every level when managing IT. Security should not be a product or add-on feature.

10. Is your company SSAE 18 compliant?

Look for: Affirmation that they comply with auditing standard for service organizations. MSPs that follow best practices themselves are best positioned to help you do the same.

11. What are the most common types of cybersecurity issues your clients deal with?

Look for: The same types of issues you're concerned about. Examples include getting hacked, ransomware, fraud, unauthorized access, brand reputation, DDoS attacks, data loss, and insider threats.

12. How do you usually handle those issues when they come up?

Look for: A commitment to follow ITIL (IT Infrastructure Library) practices. Ideally, they'll talk about consistent methodology being the key to handling security issues whenever they come up, including how to handle mega-hacks.

"Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches."

— Bruce Schneier, Schneier On Security

Cybersecurity delivery questions

13. **Talk to me about how you usually handle isolated, specific-client issues.**
    Look for: By following best practices. They should adhere to an incident management process, either ITIL or ISO (International Organization for Standardization).

14. **How do you handle security issues when they're more system-wide or impact multiple clients at the same time?**
    Look for: 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.

15. **What is your methodology to reassess our level of risk as we progress?**
    Look for: Processes that include constant re-evaluation and enhancements after having designed and deployed your improvements.

16. **Who specifically have you worked with that has had problems like ours?**
    Look for: At least one or two recent success stories and preferably plenty of examples of institutional knowledge related to your specific problem areas.

17. **What is your typical timetable for being able to improve security for your new clients?**
    Look for: A realistic approach — it's unlikely an experienced MSP that follows best practices will be able to offer a quick-secure option.

> "The old idea that cybercrime is like a business needs to be replaced with a new metaphor that better captures its internal complexities; that is, that cybercrime now has its own economy – a literal "web of profit" that not only mirrors its legitimate counterpart, but that both feeds off it and feeds into it."
>
> — Dr. Mike McGuire, Into The Web of Profit

Risk and expectation questions

18. Talk to me about the evaluation process you'll use to determine what you'll recommend for us?

Look for: 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.

19. What can you tell me about the kinds of results we can expect?

Look for: Confirmation that you can expect the same kinds of results their other clients have experienced. They should be able to provide data that show marked improvements.

20. What improvements have you made to your own security processes since last year?

Look for: Having integrated new tools, roles, and compliance standards. They should also have made adjustments based on evolving cybersecurity threats.

21. What kind of transparency and reporting do you provide?

Look for: A portal or system that catalogs your company's business policies, procedures, and compliance evidence 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.

Step Three:
Vet your options with your team

Now that you have interviewed your cybersecurity partner shortlist, rank each on the three most important factors to consider when making your final decision — which has the right people, processes, and tools to match your needs?

People:

- Do they share our business principles and seem culturally and philosophically compatible?
- Do they have the levels of experience, capabilities, and stability that we need?
- Since we'll be interfacing with the company frequently, is there natural chemistry between our people?

Processes:

- Do they follow best practices both internally and with their clients?
- Do they have an effective methodology to deliver on their security promises even when multiple clients need attention?
- Are they among the best of breed for cybersecurity?

Tools:

- Is their toolset a good match for us?
- Will they follow our company's policies and provide transparency into the state of our security program and any issues we're experiencing?
- Are we confident their team will stay on top of the most effective tools for emerging threats?

Securing your IT operations is too important to ignore

By choosing an outsourced IT partner that enables you to put the most important cybersecurity pieces in place — people, processes, and tools — your organization can feel confident moving forward. Adhering to proven methodologies is key. 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 come up (no methodology is foolproof), and limit your potential loss. Teaming up with the right partner for the long-term also helps protect your brand and attract new business.

The right IT partner also provides something intangible — peace of mind.

> "When combined into a single, integrated framework, an overlapping strategy based on security tools, people, and processes will yield the most effective defenses."
> – *A Layered Approach to Cybersecurity: People, Processes, and Technology, Fortinet blog*

Leapfrog Services is a managed IT service provider and Managed Security Service Provider (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 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 reach us at 404-870-2122 or leapfrogservices.com.