How to Choose the Right Managed Security Service Provider

compuquip

Table Of Contents

Section I

The Challenges of Managing Cybersecurity

Cybersecurity is a critical issue for modern businesses of all sizes. Failing to protect your network and data against attacks from cybercriminals can cost millions in financial losses—an average of $3.86 million according to Ponemon's 2018 Cost of a Data Breach study. Worse, a major data security breach can cost your business customers as they lose faith in your company's ability to keep their sensitive information safe.

> **"Failing to protect your network and data against attacks from cybercriminals can cost millions in financial losses—an average of"**

Yet, as important as cybersecurity is for prolonged success in any industry, many companies struggle to manage their network security strategy effectively. There are many challenges to managing cybersecurity, including:

The High Cost of Hiring In-House Cybersecurity Specialists

There is a shortage of trained cybersecurity specialists on the market compared to the demand for services—driving high wages. As of June 4, 2018, the average annual salary (not including bonuses) for a cybersecurity engineer reported by PayScale was $93,815. Considering that an entire team of such personnel would be required to effectively manage a company's network security architecture, the cost of maintaining a cybersecurity team can quickly become prohibitive.

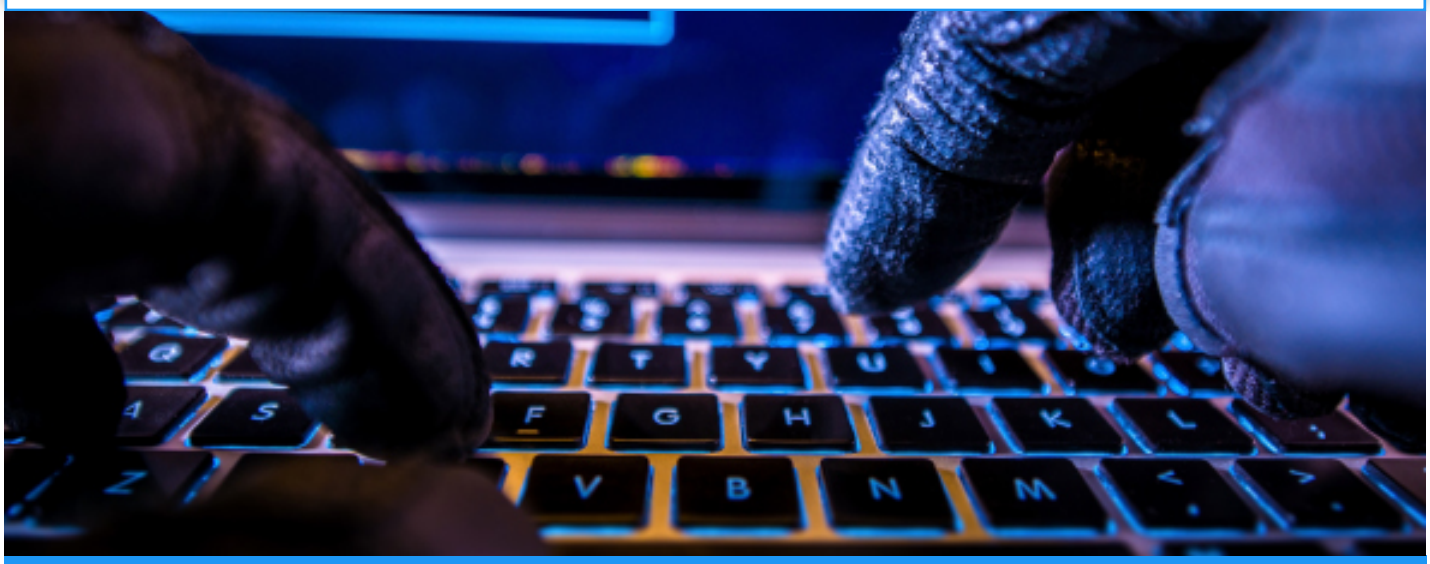
The Challenges of Managing Cybersecurity

Keeping Current on Cybersecurity Knowledge

Cyber threats are constantly evolving. Hackers across the globe create new types of cyberattacks every day, or adapt old attack methods to bypass defenses which would once work to stop them. Keeping current on cybersecurity knowledge is a must for protecting your network—but it requires constant research and effort.

Maintaining a 24/7 Response Team

Hackers don't work 9-to-5, they're up and making their attacks at all hours of the day (and night). So, cybersecurity teams need to be ready to go 24/7. To do this effectively in-house, your company would need to have at least three shifts of cybersecurity team members—with each shift covering every security specialty necessary to use all of your network security tools. Otherwise, speed of response will be limited to the next time your team clocks in (potentially giving attackers hours to do whatever they want).



Section 2

How Managed Security Service Providers Help Maximize Your Cybersecurity

A managed security service provider (MSSP) can be a priceless resource for modern companies that need to improve their cybersecurity posture, but lack the resources to handle everything internally. Some of the benefits that a top-tier MSSP can provide include:

Supplying In-Depth Cybersecurity Knowledge

MSSPs have years of experience in tackling cybersecurity challenges for a variety of companies in different industries. This helps them build a deep pool of knowledge that helps them identify, understand, and counter different cyber threats. Lessons learned from working with other companies can often be applied to benefit your organization.

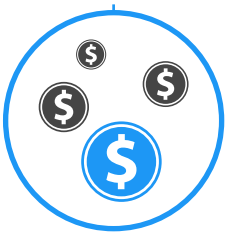
Adding New Cybersecurity Tools to Your Company

There are many times where an MSSP will know the perfect tool for closing a security gap or stopping an attack that their customer has never heard of. Using a managed security service provider helps you access new ways to protect your business.

How Managed Security Service Providers Help Maximize Your Cybersecurity

Freeing Up Your IT Team to Focus on Core Business Tasks

By bringing an outsourced team of cybersecurity specialists on board, you can free up your internal IT team to focus on other tasks—such as providing tech support or troubleshooting user interfaces for your company's software.



Reducing Cost of Labor for Cybersecurity Management

Outsourcing your cybersecurity management to an MSSP can save you money while providing more expertise. Having an outsourced team is often a fraction of the cost of maintaining and internal security team—especially after you factor in the cost of bonuses, employee training, and other expenses.

However, while using an MSSP can provide numerous benefits, that's only when you're working with the right one. It's important to choose the best MSSP to meet your company's cybersecurity and operational goals.

With that in mind, we've outlined a few advice on the next few pages to help you choose the right managed security services provider for your company.

> **MSSPs have years of experience in tackling cybersecurity challenges for a variety of companies in different industries. This helps them build a deep pool of knowledge that helps them identify, understand, and counter different cyber threats.**

Section 3

How to Choose an MSSP: Setting the Criteria for Selection

> **...the criteria you set should be tailored to your business's specific needs..**

The first step in choosing a managed security services provider is setting some basic criteria for the selection. When setting selection criteria, you can be as detailed or as general as you want. However, the criteria you set should be tailored to your business's specific needs. For example, if you're a healthcare provider, then odds are that your MSSP needs to be cognizant of the Health Insurance Portability and Accountability Act (HIPAA) and how to meet it.

Some examples of MSSP selection criteria could include:

Knowledge of Specific Cybersecurity Technologies

Does your business use a particular cybersecurity tool already? One criteria for selection you might set is that the MSSP be familiar with that particular technology. Of course, it may be difficult to find an MSSP who knows particularly esoteric or rare security tools, so it may come down to their willingness to learn the system (or ability to provide a reliable alternative).

How to Choose an MSSP: Setting the Criteria for Selection

Service Level Agreements (SLAs)

What SLAs does the MSSP have to be able to fulfill to meet your business's security needs? What kind of incident response time, time-to-resolution, and incident reporting goals does your company require for optimal protection? Consider setting SLAs and seeing if your MSSP is able to meet or beat them reliably.

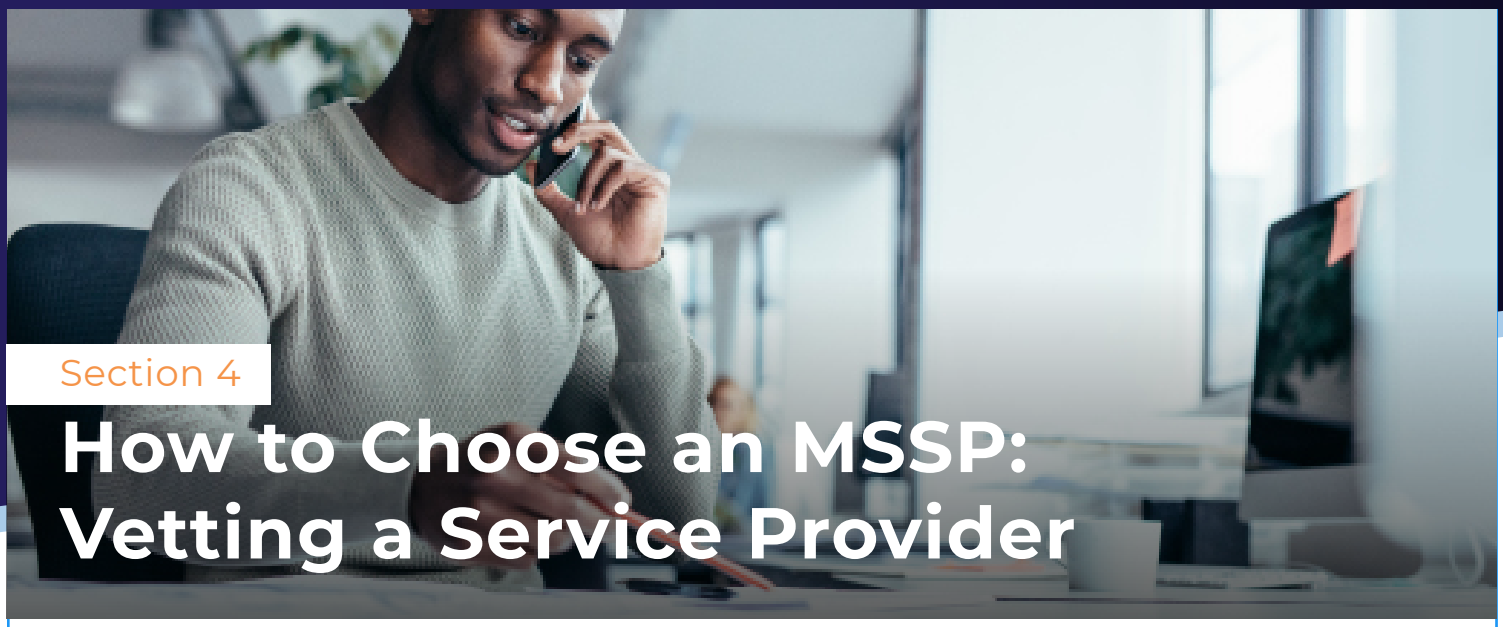
Ability to Hold Meetings to Discuss Security

Will the MSSP make time to meet with you or your IT team to discuss their cybersecurity strategy or recent events impacting your company's network security? Being able to regularly meet with your MSSP—either in person or over the phone—is crucial for keeping in the loop so you can control the direction of your cybersecurity efforts. It can also help demonstrate the return on investment that your company is getting from the MSSP as they demonstrate how they are protecting your business.

The Ability to Offer Specific Cybersecurity Services

Some MSSPs have different specialties that may or may not be needed by your company. For example, one company may specialize in firewall management, but lack expertise in cloud security issues. Another company may work exclusively with one operating system (OS), but not others—such as working only with iOS devices and not Windows devices or vice versa. It's important to check what types of services the MSSP can offer as well as what specific operating systems they have experience in.

Remember, when setting these criteria, it's important to customize each one to your company's goals and needs. Keeping in mind the requirements of specific industry regulations affecting your business can help you create better selection criteria that will help you find a reliable MSSP to partner with.



Section 4

How to Choose an MSSP: Vetting a Service Provider

So, you've created a solid set of selection criteria to find the perfect MSSP to meet your business's needs. However, how can you be sure that they're a good fit? They may claim to satisfy all of your selection criteria, but it's important to verify those claims before entering into a long-term service agreement.

How can you verify that your MSSP can "walk the walk?" A few simple tips include:

Checking with Security Solution Vendors to Verify Certifications

Did you know that Compuquip is a 4-Star Elite Partner of Check Point Software Technologies? It's a partnership our team worked hard to cultivate so we could use their incredibly useful network security solutions to the fullest. However, you shouldn't take our word for it—you should reach out to Check Point directly and verify it for yourself.

Why?

Because, anyone can simply slap a security solution vendor's logo on their website page and claim to be certified for that vendor's products—at least until they're caught and forced to remove the logo. One way to protect your business from bogus resellers and service providers claiming false expertise is to reach out to the security solution vendor and check if the MSSP actually has a certification from the company.

If you're making expertise in a particular security tool one of your selection criteria, then it is especially important that you do this.

When vetting an MSSP's certifications, you can easily find the certifying organization's information online. However, it is important to avoid relying on links on the MSSP's own site for this, as an unscrupulous company may link to a fake site to provide a false certification.

How to Choose an MSSP: Vetting a Service Provider

Checking the MSSP's References

Is the managed security services provider willing to provide references from current and past clients? Are there online reviews of the company that you can read?

Putting in some time to track down some other companies to act as references for the MSSP can provide you with priceless insight. These references can let you know exactly how the MSSP treated them—and thus, how they're likely to
treat you.

Try to collect information from as many sources as possible. Any one customer could be an outlier—whether positive or negative. Getting a few reviews from different sources can help you get a better idea of how the service provider works and whether they'll do their best to help you.

Verify How the MSSP Will Handle Your Data

It's kind of ironic, but not even cybersecurity companies are immune to cyberattacks. Cybercriminals may attack an MSSP for the challenge or to access sensitive data on their clients. So, it's important to be sure of how they will handle and process your company's data.

Some concerns about the way the MSSP will handle your data include:

- Where/how the data is stored
- Whether the data is encrypted
- What security measures the MSSP uses to restrict access to the data
- Whether the MSSP has a backup of the data in case of disasters

Verifying these details can help to protect your business against data breaches and data loss.

How to Choose an MSSP: Vetting a Service Provider

Ask the MSSP How Willing They Are to Adopt New Security Solutions

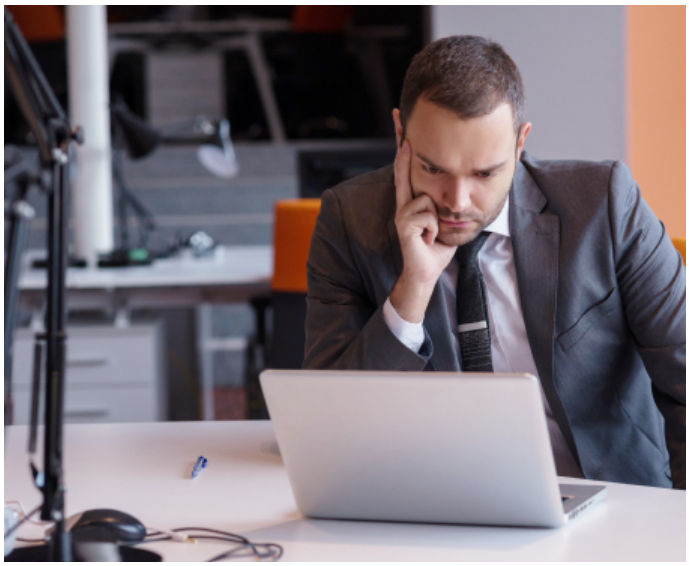
Does the managed security provider not have expertise in the security tools that your business uses? Are they willing to learn your solutions or are they dead set on using a single standardized security package that they use for every customer they have, regardless of industry?

Getting the answers to these questions can be crucial for determining whether a given cybersecurity partner will be a good fit for your business. If the MSSP doesn't know your security tools, and isn't willing to learn them at all, then they may not have the flexibility needed to create a personalized cybersecurity plan that maximizes network security for your business.

However, there may be times where a cybersecurity company may recommend discarding a specific cybersecurity tool because they know of a better alternative.

> **"If the MSSP doesn't know your security tools, and isn't willing to learn them at all, then they may not have the flexibility needed to create a personalized cybersecurity"**

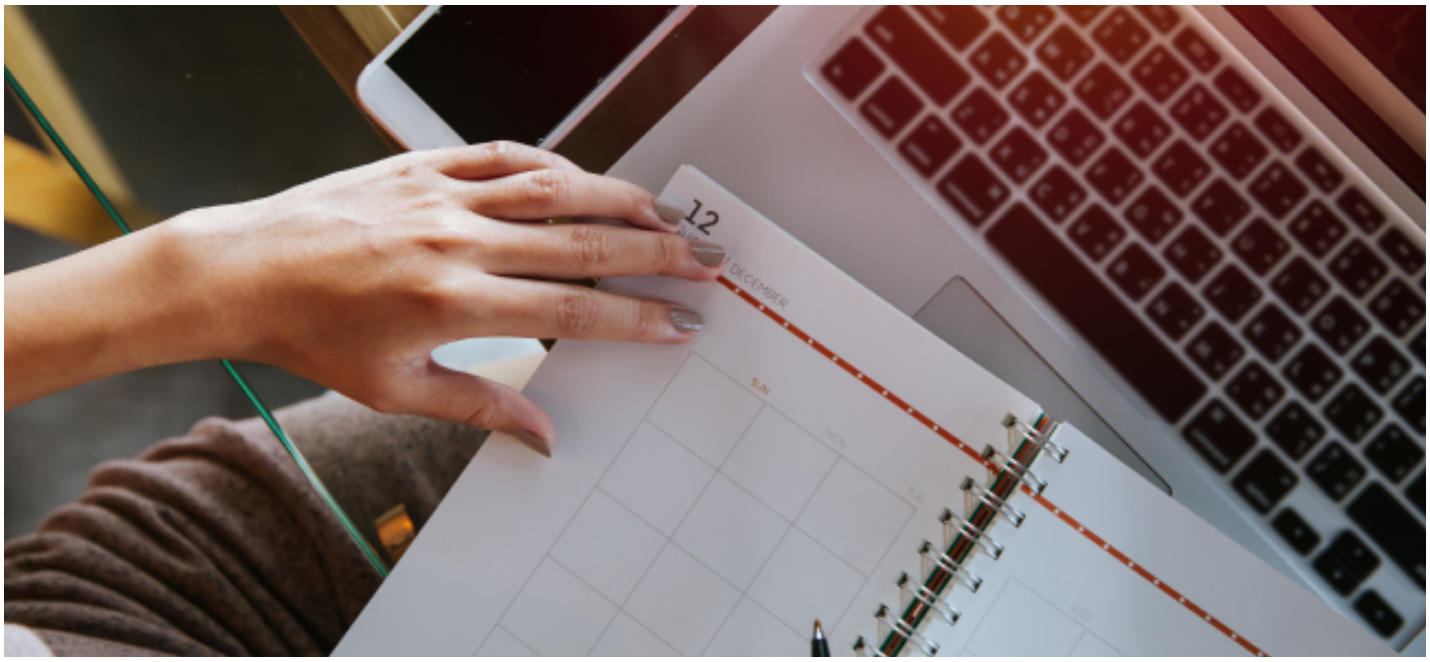
Testing the MSSP's Cybersecurity Knowledge



It's crucial that you know you can rely on the expertise of your managed security services provider. One way to verify this is to run some tests on their cybersecurity knowledge. This can be done by making them pass a cybersecurity knowledge course from an online learning platform or by conducting an interview.

Most companies prefer the online testing course because it's easier to set up and to check the results. On the other hand, having an interview with the MSSP can be beneficial because you can get a feel for their expertise and even learn something you might not have known before.

How to Choose an MSSP: Vetting a Service Provider



Setting up Communication Guidelines

When partnering with an MSSP, it's important to set some expectations for how (and how often) they'll communicate with you. Being able to talk to your MSSP is crucial because it keeps you up-to-date with the latest information regarding the state of your cybersecurity.

Obviously, one of the reasons to adopt an MSSP in the first place is to reduce the time and effort you have to spend on managing your network security. So, odds are that you won't want to spend too much time on meetings with your security service provider. However, regular communications, such as a weekly meeting, can help you stay on top of your network security strategy with a minimum of effort.

Other ways to communicate with an MSSP include regular status report emails, emergency text communications (for when they spot a security breach or other critical issue), and even in-person meetings.

If an MSSP is not willing to set a communication schedule with you, that may be a warning sign of how they'll treat the "partnership" later.

Vetting a service provider is crucial for choosing the right one for your needs. However, what's next?

Section 5

Next Steps/Why You Might Want to Partner with Compuquip for Cybersecurity

So, if you're wondering why you might want to use Compuquip's managed security services, here are a few reasons:

We Have a Long History of Success as an MSSP

Compuquip got its start way back in 1980 as a banking equipment leasing company and grew over the years to add maintenance, installation, and managed security services. At every step of our growth over the last few decades, we have consistently earned the praise of our customers for our commitment to doing things right and providing top-notch service.

Co-Managed Solutions that Don't Take Away Your Control

Many of Compuquip's cybersecurity services are available in co-managed models that allow customers to retain a high degree of control while still benefiting from our many years of experience. We're more than happy to work with you and even provide your internal cybersecurity team the training they'll need to take control of your network security strategy.

Next Steps/Why You Might Want to Partner with Compuquip for Cybersecurity

"Cloud First" Strategy to Minimize Infrastructure Demands

Many cybersecurity companies rely heavily on clunky and difficult-to-deploy hardware-based solutions that take time and money to install. Compuquip applies a "cloud first" strategy to minimize the need for hardware that you have to install and maintain—saving you time and money while improving your cybersecurity faster.

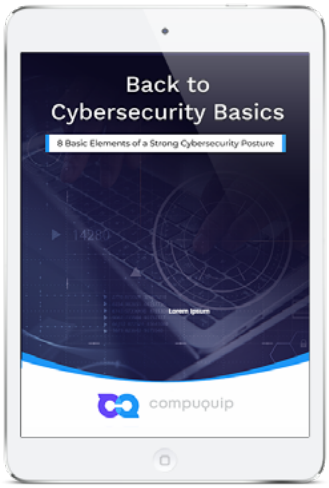
Willingness to Learn New Security Solutions

Compuquip applies a "technology-agnostic" philosophy to our managed security—meaning we aren't tied to any one solution. We'll adapt to and adopt new security solutions as needed. Then, we'll strive to earn the highest level of certification possible for these security solutions. For example, we are a 4-Star Elite Partner for Check Point and a top-class Florida Rapid7 Partner.

Are You Ready to Partner with an MSSP Who Cares about Your Needs?

You can reach out to our Chief Information Security Officer (CISO), Michel Ramirez today to learn more about Compuquip and how to perfect your cybersecurity strategy. Or, you can contact us at:

CONTACT US TODAY



Back to Cybersecurity Basics

8 Basic Elements of a Strong Cybersecurity

DOWNLOAD NOW

Email: info@compuquip.com

Phone: 789-641-5437

Address: 2121 Ponce De Leon Blvd. Suite 530
Coral Gables, FL 33134

Follow us on: