Guide for Small and Medium-sized Businesses

When and How to Get Outside Cybersecurity Support

CYBER READINESS INSTITUTE

Release Date: December 2025

Table of Contents

Should I Get Outside Support to Manage My Cybersecurity Risk?

Introduction

If you are like most small and medium-sized business owners or managers, you wear many hats. Your focus is usually on the fundamentals of managing and building your business. You know that cybersecurity is an area of growing risk because there's been more news about it — especially more news about ransomware and phishing attacks. You wonder if you are doing enough to protect your organization or if you should get outside help.

Effective cybersecurity requires the right mix of people, process and technology. Yes, technology like virtual private networks (VPNs) and antivirus software helps, however you also need a workforce that is aware of the basic elements of cybersecurity. After all, it just takes one misguided click on a phishing link to potentially bring down your operations.

There was a time when cybersecurity was not considered to be a "fundamental" of managing an organization — that time has passed. You need to focus on it the same way you prioritize your financials, customer relations, and human resources. From the last few years of cyber-attacks and breaches, we have learned that you must not wait until disaster strikes to pay attention to cybersecurity.

Maybe in the past you thought you wouldn't be a target for hackers. Now it's clear that hackers are using AI to attack small and medium-sized businesses (SMBs) more frequently with ransomware for financial gain, as well as using small companies as gateways to attack larger businesses.

You realize you need to do something, but you're not sure what you should do or if you need outside help. It may sound overwhelming. Remember, you can outsource some of your cybersecurity responsibilities and tasks, but **you cannot outsource your accountability for cybersecurity.** With or without outside help, it will always be your responsibility to create and foster a culture of cyber readiness within your organization.

> The **Cyber Readiness Institute** focuses on practical steps you can take to influence human behavior and create a culture of cybersecurity. This guide will help you through the process of determining if you need outside help, what kind of vendor may be best, and how to manage them to get the most value. Our **free online Cyber Readiness Program** guides small and medium-sized business to take practical steps to become cyber ready.
>
> **TO LEARN MORE:** Cyber Readiness Program

Getting Started: Identify Your Crown Jewels

The first step is to take an honest look at your cybersecurity risk and prioritize the data and systems you need to run your organization. Here are some quick tips to get started:

1. **List the information and data** that is most important to the success of your organization (e.g., customer information, confidential business information).

2. **List the computer hardware** that is most important to run your organization. Consider information technology (e.g., computers, laptops, tablets, smart phones), and operational technology if relevant (e.g., computer-controlled machinery, process controllers).

3. **List the information technology (IT**) and **operational technology (OT) software** that is most important for running your organization (e.g., operating system, word processing, spreadsheet, email, file storage, accounting, databases).

4. From the lists above, **identify the top three to five items** that would cause the most damage to your organization if they were unavailable, lost or stolen. Let's call these your crown jewels.

5. **Identify who has access to your crown jewels.** Consider employees and contractors and whether they are using company-issued hardware or using their own devices. Also consider suppliers and customers.

6. **Realistically determine how well protected** your crown jewels are — and — if you're comfortable with the level of protection.

7. **Determine if there are any data protection, cybersecurity, or data privacy requirements** from your customers or applicable federal or local laws and regulations.

DEFINITIONS:

Information Technology (IT) encompasses the tools and processes used to manage electronic data. It involves the use of computers, software, and networks to gather, store, process, and share this data securely and efficiently.

Operational Technology (OT) is the integration of hardware and software dedicated to monitoring and controlling physical devices and processes within industries such as manufacturing, energy, and telecommunications. It employs specific technologies like Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) to manage, monitor, and automate industrial operations in real-time.

Protecting Your Crown Jewels: Do You Need Outside Support?

If you can't tell how well protected your crown jewels are, *you need outside support.*

If your crown jewels need better protection and you don't know what to do, *you need outside support.*

If you are unclear about relevant data protection and data privacy regulations, *you need outside support.*

Don't worry if it looks like you need to get outside support. Most SMBs get some outside support for managing their IT, OT and cybersecurity. As a non-profit organization, we're here to give you free, straightforward advice. We can help you understand the difference between an IT consultant, a Managed Service Provider (MSP), a Managed Security Service Provider (MSSP), a virtual Chief Information Officer, and a virtual Chief Information Security Officer.

When assessing your cybersecurity risk, think about data loss and business continuity and what the impact would be. Is one scenario much worse or are they equally bad?

DATA LOSS

Imagine you can't access any of your data, your data is corrupt and not usable, or your confidential data is made public

BUSINESS CONTINUITY

Imagine the hardware and software you use to run your organization is shut down

If you're an accounting firm, losing customer data is probably a lot worse than having your website go down for a week. If you sell products online, having your website go down for a week could be extremely costly.

An Introduction to Outside Vendors that Offer IT and Cybersecurity Support

Looking for Help

Like many small businesses, you've come to the conclusion that you need outside information technology (IT) and cybersecurity support. If your business uses operational technology (OT) your need for outside support is even greater — especially with the increase in AI-enabled attacks.

You realize that IT and cybersecurity are becoming business management "fundamentals" — like finance and sales. But you don't have the time to figure it all out. If you're like most SMB owners or managers, you may not be sure what kind of support you need or even what questions to ask. There are many different types of cybersecurity vendors that offer to help, ranging from individuals to large companies.

As the threat of cyber-attacks has escalated, so have the number and types of companies offering their assistance. AI has made the situation more challenging because it is a friend and a foe in cybersecurity. It has increased the sophistication of cyber-attacks but also provided advanced technology to detect and prevent attacks. It is a confusing market with overlapping service offerings and more acronyms than you can imagine.

Regardless of who you contract to help, always remember that **ultimately you are responsible** for the cyber readiness of your organization. You can outsource certain IT activities, like installing software updates, but you are accountable for setting the policies, building a cyber ready culture, and satisfying any privacy and security compliance obligations.

Getting Support to Hire the Right Vendor

It may sound odd, but you may want to consider hiring a consultant to help you pick that right type of vendor. One of the first decisions is whether you want to hire a trusted advisor to guide you through the process or wade through the vendors on your own. We know that the idea of hiring a consultant to pick the right vendor(s) can seem like an added expense. However, it may be less expensive in the long run because they can ensure that you are getting the services you need at a fair price. If you decide to go this route, make sure that the consultant you hire is independent and not tied to any vendor, or not competing to become your ongoing IT consultant.

Types of IT and Cybersecurity Support Vendors

Here is a list of the types of companies you'll encounter and a brief description. Remember there will be some overlap in the types of service they provide. Depending on the size or your organization and your cybersecurity risk, you may end up hiring more than one type of vendor.

IT and/or OT Consultant

IT and/or OT Consultants are general purpose helpers. They may be an individual or a small firm. Generally speaking, the IT Consultant will help set-up and operate the IT or OT systems. Typically, they assist with setting up your networks, devices and/or Wi-Fi, recommending and installing software, setting up emails and user accounts, creating and testing backups, and more.

Managed Service Provider (MSP)

MSPs are typically small firms that offer similar services to IT consultants plus more advanced monitoring and ongoing management of the overall IT systems. Recently, there has been a trend toward creating larger MSPs through acquisition. They often are certified installers or advisors of several hardware and software vendors. Some MSPs say they specialize in cybersecurity, meaning their services would overlap to a greater extent with those of an MSSP.

Managed Security Services Provider (MSSP)

The MSSP will verify that the IT Consultant or MSP is building and maintaining the network to maximize value and reduce cyber risk reduction since some MSPs and IT Consultants have limited knowledge about cybersecurity technology or monitoring. MSSPs often perform activities like penetration testing, intrusion mapping, log monitoring, risk assessment, threat detection, planning and consulting, policy compliance, and incident response plan testing.

Virtual Chief Information Officer (vCIO)

For businesses that may need a part-time CIO within their workforce, vCIOs offer a way for you to outsource the function, like outsourcing the General Counsel or Chief Financial Officer functions. This approach tends to be for organizations that are a little larger on the small to mid-size scale. vCIOs will manage,

More on How to Distinguish Between the Vendor Types

It's common to confuse the types of vendors and there is often overlap. But these roles serve different purposes. MSPs provide outsourced IT or OT services, focusing on specific tasks, whereas a vCIO takes on a more proactive, strategic role in driving long-term IT and OT initiatives. CIOs also collaborate with a company's management team to guide IT budgeting, while MSPs work within the provided budget to deliver services.

A virtual Chief Information Security Officer (vCISO) is a security professional who provides cybersecurity leadership and expertise on a part-time or project basis. They can help with cyber risk management, incident response testing, technology evaluation and more.

implement, and recommend products and services to improve your IT systems and security levels. They will help to select and coordinate with all relevant outside IT or OT vendors.

Virtual Chief Information Security Officer (vCISO)

A vCISO is a part-time security expert who provides strategic cybersecurity leadership and guidance to organizations that don't require a full-time CISO. vCISOs are more specialized in cybersecurity than vCIOs offering expertise in risk management, cybersecurity policy and procedure development, incident response, and cybersecurity technology implementation.

Relevant Professional Credentials

Here's a partial list of the common and respected types of certifications or professional credentials you may encounter when assessing vendors who provide outside support.

CISSP – Certified Information Systems Security Professional

This is a globally recognized advanced certification that covers a wide range of cybersecurity topics, with a focus on technical knowledge. It requires a minimum of five years of full-time work experience, extensive technical knowledge and passing an exam.

CISM – Certified Information Security Manager

This globally recognized certification focuses on cybersecurity governance and risk management and less on technology than CISSP. It requires 5 years of relevant professional experience. Those who have obtained this credential typically manage security at the organizational level (e.g., CISOs).

CompTIA Security+

A basic cybersecurity certification that provides a good foundation for those seeking more advanced professional credentials.

Specialized Credentials (depending on need):

SANS Institute

SANS Institute offers a variety of technical certifications, divided into focus areas such as Cloud Security, Penetration Testing, Ethical Hacking and Security Management, Legal and Audit. The SANS GIAC Security Essentials (GSEC) certification signifies that the individual has a foundation of broadly applicable knowledge and specific technical skills.

CISA – Certified Information Security Auditor

This credential is for individuals qualified to take a risk-based approach to audit, monitor and assess IT technical systems and management systems. Continuing education requirements help ensure the person stays current, including with the application of AI.

CIPP – Certified Information Privacy Professional

This credential is for individuals qualified to evaluate an organization's compliance with data privacy laws. There are specific certifications based on the laws in the EU, US, Canada and Asian economies.

CEH – Certified Ethical Hacker

This credential, offered by the EC Council, means the individual has learned how to think like a hacker, but use those skills to protect and prevent attacks, as opposed to penetrating a system with malicious intent.

How to Select the Right Level of Outside Support

FOUR STEPS TO SELECTING A VENDOR

Now that you understand your options, you're ready to learn how to select the best type of vendor for your specific needs. We recommend you take a risk-based approach. These questions will help you better assess and understand your cybersecurity risk.

Step 1 of 4: Determine Your Level of Cybersecurity Risk

1. Do you collect and store Personally Identifiable Information (PII) of your customers (name, email, address, social security number, age, gender, etc.)?
a. Yes
b. No

2. Do you collect and store Personal Health Information (PHI) of your customers (name, medical history, medical test results, prescriptions, etc.)?
a. Yes
b. No

3. Do you collect and store any financial information of your customers (credit card numbers, bank accounts, etc.)?
a. Yes
b. No

4. Do you have valuable confidential information from your organization or the organizations you work with on your computers?
a. Yes
b. No

5. Would your business be seen as an attractive gateway for hackers to access your customers or suppliers?
a. Yes
b. No

6. How damaging would it be to your organization if the information on your computer systems was lost or made publicly available?
a. Extremely damaging
b. Damaging
c. Not very damaging

7. How damaging would it be to your organization's operations if your computer systems were unavailable for 72 hours (three days)?
a. Extremely damaging
b. Damaging
c. Not very damaging

8. How damaging would it be to your customers or the community if your data was unusable or you were unable to operate?
a. Extremely damaging
b. Damaging
c. Not very damaging

> If your answers to the above are mostly **"yes"** your organization has a high level of cybersecurity risk. If you selected **"damaging"** or **"extremely damaging"** for data loss and business continuity, your risk is even higher.

Step 2 of 4: Determine Your Current Capabilities

1. Do you currently have a person in your organization that is responsible for setting up and managing your computers and software?
a. Yes
b. No

2. Do you currently have a person in your organization that is knowledgeable about cybersecurity threats and prevention?
a. Yes
b. No

3. Do you currently have a contract with an outside consultant or firm to set-up and manage your computers and software or help with cybersecurity?
a. Yes
b. No

4. Do you have a clear understanding of who is responsible for basic cybersecurity policies and practices in your organization (passwords, use of multi-factor authentication, software updates, etc.)?
a. Yes
b. No

5. Do you have a person responsible for training your workforce on following cybersecurity policies?
a. Yes
b. No

> If the answers to the above are mostly “**no,”** your organization should hire a vendor to help you improve your cybersecurity.

Step 3 of 4: Determine the Type of Support Needed

There are hundreds of companies and individuals willing to provide outside IT and cybersecurity support to you. Knowing how to identify the best outside company to address your business needs is a challenge. IT Consultants or MSPs may not have the proper training and experience needed to address your unique cybersecurity requirements. MSSPs, vCIOs or vCISOs may encourage you to adopt sophisticated technical solutions.

The key for you is to take a risk-based approach and engage with a vendor appropriate for your risk level. It’s not the size of your company that matters; it is your level of risk.

Step 4 of 4: Select a Cyber Leader in Your Organization

Regardless of what type of vendor you hire, you must have an internal champion for cybersecurity — your Cyber Leader. The Cyber Leader builds a culture of security and ensures associated safeguards are implemented with the support of senior management and the outside vendor. The Cyber Leader is the point person between your company and the vendor.

> The **Cyber Readiness Institute's free online Cyber Leader Certification Program** is a personal professional credential that can be achieved after completing the Cyber Readiness Program. This management program shows how people, process and technology work together to create and sustain a cyber ready culture in your organization.
>
> **TO LEARN MORE:** Cyber Leader Certification Program

Understanding Your Cybersecurity Vendor Service Agreement

At this point in the process, you have decided to use outside support to improve your cybersecurity. We've provided you with guidance on the various types of service vendors.

In this section, we provide insight into the operational elements you should consider and the questions to ask to see if it is a good fit. Warning – we do not provide legal advice, and you should consult a lawyer if you have any legal questions. Beyond its legal aspects, the agreement is a critical document in defining exactly what services will be provided and your ongoing responsibilities for cybersecurity.

We suggest you use the agreement as a checklist to make sure that you and your vendor have a mutual understanding of responsibilities going forward. You will want to make sure all your expectations are addressed. Don't fall into the trap of waiting until there is a breach to understand what is and isn't covered in the contract. At that point it's too late to do anything.

We suggest you have a quarterly review with the vendor using the agreement as a checklist to assess how the relationship is serving your organization's needs. Cybersecurity threats evolve rapidly, and you want to make sure you and your vendor are proactively implementing preventative measures to be secure and resilient.

It is important that you develop a trusted relationship with your vendor. Ideally, the vendor will become part of the team helping your organization build and maintain a functional and secure IT and/or OT capability. Understanding the contract and vendor responsibilities are critical to establishing trust from the beginning.

We have broken this section into two parts:

- **Pre-Contract Review**
- **Service Checklist**

Pre-Contract Review

Agreements with cybersecurity vendors may have up to three components depending on what they are doing for your organization and their internal processes:

- **Service Level Agreement (SLA):** Outlines the specific support services to be provided, the expected response times, and the consequences if the vendor fails to meet the agreed-upon service levels. It defines the priority levels of support requests, and the associated response times.
- **Statement of Work (SOW):** Outlines the specific work to be performed by the vendor for a particular project. It is typically used for one-time projects, such as software upgrades or network installations. An SOW clearly documents the products and/or service included in the project and the deliverables.
- **Master Services Agreement (MSA):** Establishes the overall terms and conditions of the relationship between the vendor and your organization. It outlines the general scope of services, pricing, and payment terms, as well as any other important considerations, such as liability and confidentiality. An MSA is often used as the umbrella agreement for long-term, ongoing relationships and SOWs are signed under the MSA.

Before entering a detailed discussion of the contract, it is important to learn about your potential vendor's background and experience. These are some key screening questions. There are no "correct" answers to the following questions: they are intended to help you understand the level of sophistication of your vendor.

Initial Screening Questions for Your Possible Vendor

1. If we work with your firm, **who will be the primary relationship manager?** What is their background?
2. **Who else is on the service delivery team** for my organization? What are their roles and backgrounds?
3. **Do you perform background security checks** on your employees?
4. **Do you have cybersecurity insurance?** To what extent does your insurance cover cybersecurity damages at my organization? Does it specifically cover a ransomware attack at my organization?
5. **What are the normal hours of support** during the work week and on weekends?
6. **Do you provide 24/7 emergency support** and is it part of the standard contract?
7. For the services we are contracting you to deliver, **will you be using sub-contractors**? If so, for what services?
8. **What security controls do you maintain** and are they aligned with any standards or frameworks (such as NIST 800-53, NIST Cybersecurity Framework, ISO27001, SOC2, etc.)?
9. Are you part of any organization or service that **provides you with cyber threat intelligence?**

Service Checklist

Once you get beyond the initial screening, it's time to get into the specifics with the leading candidates. Here are questions you can use to evaluate your needs and if the possible vendor is going to be a good fit. You can use the answers to shape the service agreement. Use this list as a general guide because you may not need all these services.

✓ Understanding and Fit

- Do they understand your business operations and size?
- Have they supported small businesses in your industry?
- Can they explain services in plain language?
- Do they support both IT and OT systems (if needed)?
- Do you get a dedicated contact?
- What's their typical response time?

✓ Core IT Services

- Do they offer 24/7 support or business hours only?
- Do they manage software updates and patches?
- Do they monitor network/server health proactively?
- Can they help set up or manage cloud services?
- Do they handle hardware/software purchasing and setup?
- Do they support remote workers securely?
- Do they document your systems clearly?

✓ Cybersecurity (MSSP)

- Do they provide 24/7 threat monitoring and response?
- Do they include firewalls, antivirus, and intrusion detection?
- Do they offer regular security reports?
- Can they implement MFA and encryption?
- Do they assist with incident response planning?
- Have they worked with compliance frameworks (SOC 2, NIST, CMMC, etc.)?
- Do they have OT cybersecurity experience?

✓ Backup & Recovery

- Do they provide automated, off-site backups?
- Are backups tested regularly?
- Can they restore systems quickly?
- Do they have clear recovery time goals?
- Do they include OT systems in recovery plans?
- Do they offer business continuity planning support?

✓ OT & Industrial Systems

- Do they understand IT vs. OT network separation?
- Can they secure OT systems from IT network cyber threats?
- Do they have experience with ICS, PLCs, SCADA, or IoT?
- Do they monitor OT network activity and security?
- Can they coordinate with machine/equipment vendors on your behalf?
- Do they perform OT-specific cybersecurity risk assessments?

Reporting & Communication

- Do they provide regular performance/ security reports?
- How often do they review results with you?
- Can they explain results in business terms?
- Do you have full access to configurations and passwords?
- Are pricing and scope clear in the contract?
- Can you adjust or cancel easily if needs change?

Pricing & Value

- Is pricing flat-rate or time-based?
- What’s included and what costs extra?
- Do they charge per user, per device, or per service?
- Are security tools bundled or separate?
- Can services scale with business growth?
- Do they provide cost-saving examples or references?

Cybersecurity Strategic Planning

- Will they help create a technology and cybersecurity roadmap?
- Do they review and recommend new cybersecurity technologies?
- Can they support digital transformation projects?
- Do they stay current on cyber threats?
- Do they assist with compliance or certifications if needed?

Managing the Relationship with Your Cybersecurity Vendor

Today, almost every business is digitally connected to their customers and to other businesses. Small restaurants have online ordering. Small accounting firms use cloud-based software or file sharing with their clients. Email and texting are ubiquitous for every type of organization.

As a result, the relationship you have with your cybersecurity vendor is as important to your business as the relationship you have with your accountant or bank. It is in your best interest to treat the relationship as a priority and seek to have the outside support vendor become a trusted partner. Technology is rapidly advancing, and cybersecurity threats are always evolving. You need to build an open and transparent communication channel with your vendor.

The first year is critical for building the foundation of a long-term relationship. Don’t sign the contract and forget about it. Use the contract as the basis for establishing clarity about your respective responsibilities going forward. We recommend that you set up monthly meetings during the first quarter and consider scheduling a check-in call at least once every three months in the first year. Use the check-in call to educate yourself about what they are doing for your organization. Ask them about new cybersecurity threats, trends in protective technology and the use of AI. Review your responsibility and their responsibility for cybersecurity. Remember, ultimately you are responsible for the human behavior in your company. By establishing a regular review with your vendor that has cybersecurity on the agenda, you send the message that cybersecurity matters to you. The goal is to create an open, trusted communication channel so your outside support firm becomes a partner with you.

One of the things you can do to make the most of the vendor relationship is to identify an internal colleague that is responsible for managing the relationship. Have that individual (the Cyber Leader) pursue the CRI Cyber Leader Certification which includes guidance on managing the vendor relationship.

The relationship you have with your vendor is one of the most important relationships for your organization. We hope that this guide has helped you to identify the right level of service, select the right type of firm, and learn how to manage the relationship.

Tips for Building the Relationship

- **Be proactive** in the relationship.
- **Encourage your vendor to anticipate** your operations and related cybersecurity needs.
- **Build trust by engaging** in back-and-forth communication, even if you don't have physical proximity or locality.
- **Be clear on the boundaries** of their cybersecurity responsibility. You always have a role in your cybersecurity.
- **Don't be confused by technical language**. If you don't understand something the vendor is telling you, ask them to explain it in a less-technical way.
- **Request current information** on service utilization (i.e., number of helpdesk tickets, number of accounts set up, date of last software update, utilization of multifactor authentication, etc.).

CYBER READINESS INSTITUTE

cyberreadinessinstitute.org