

Step 2: Consider Hiring an Advisor

Ask yourself the following questions about whether or not additional support is a logical move for your business.

Do I have to comply with regulations?

Yes No

Do I interact with employee information, customer Personally Identifiable Information (PII) or Protected Health Information (PHI)?

Yes No

Is my business located in a state with privacy laws?

Yes No

Am I fully informed of the requirements and expectations my customers have?

Yes No

Do I accept credit cards as payment?

Yes No

Am I part of a critical infrastructure supply chain?

Yes No

If the answers to the above are mostly “yes,” then an Information Security/Cyber Advisor/Virtual Chief Information Security Officer (vCISO) would likely be helpful for you. They can provide additional support to guide you through the process of selecting outside support.

If the answers to the above questions are mostly “no,” you may not need outside help determining what outsource services are needed.

Step 3: Distinguish Roles

There are hundreds of companies and individuals willing to provide outside support to you. Knowing how to identify the best outside company to address your business needs is a challenge. Many consultants may not have the proper training and experience needed to address your unique security requirements.

Managed Service Provider (MSP)

The cost of MSPs can range from \$75-\$200 per hour. Some charge a flat fee as opposed to an hourly rate and others charge based on the number of computers or people.

Virtual CISO (vCISO)

The amount of time needed and fees vary, but the cost of hiring a vCISO could be as little as a few hundred dollars a week.

Step 4: Select a Cyber Leader

The Cyber Leader builds a culture of security and ensures associated safeguards are implemented with the support of senior management and the vCISO. The Cyber Leader is the point person in your company between MSP and vCISO, if you've engaged a vCISO.

Step 5: Determine Your Requirements

The following table lists some of the more common requirements and actions with which you might need assistance. As you are distinguishing between MSPs and vCISOs, use the checkboxes below to indicate which items are relevant to your business.

If you have trouble understanding the terms and concepts in the righthand column, you should discuss them with your MSP or strongly consider hiring an Advisor to help you.

MSP

- Setting up a network in a facility
- Setting up a network in an office
- Setting up a remote network
- Setting up computers for new users
- Setting up email accounts
- Installing and maintaining endpoint detection and response (antivirus) software
- Performing data backups
- Testing backups
- Establishing multifactor authentication
- Setting up a VPN
- Installing and maintaining/patching software
- Defining/implementing cloud services
- Providing help desk support
- Implementing firewalls based on your network architecture
- Determining relevant data privacy regulations (e.g., GDPR, CCPA)

vCISO (Information Security Advisor)

- Evaluating/comparing offerings from MSPs
- Creating an incident response plan
- Monitoring access, firewall, and other logs and responding to anomalies
- Tracking attack attempts
- Conducting network penetration tests
- Establishing acceptable use of personal devices
- Establishing password and other standards
- Ensuring systems are getting patched quickly and properly
- Defining technical requirements and specifications, such as for VPN, firewall, other security safeguards (controls), network architecture, and/or cloud services
- Conducting vendor risk review
- Ensuring that computers are non-addressable from outside the network
- Supporting company management in shaping culture
- Defining security implications of cloud service vendors, provide standards
- Defining and implementing methods to control access to systems and information so that authorized users have access to what they need and no more
- Aligning controls to meet relevant data privacy regulations

If most of your boxes in the left column are checked, you should hire an MSP. If most boxes in the right column are checked, you should hire a vCISO.

If your boxes were evenly split, and you have some checked in both left and right columns, consider hiring both.