How to Select the Right Level of Outside Support

This is the third in a five-part series on using outside firms to reduce your cybersecurity risk.

If you are reading this guide, you have likely reviewed our first guide in this series, “Should I Get Outside Support for Managing my Cybersecurity Risk?” and determined that you should indeed seek some form of outside support. Your next question might have been: What are the various choices when it comes to outside support? To answer that, please refer to our second guide in this series, “An Introduction to Outside Firms that Offer IT and Cybersecurity Support.”

Now that you understand your options, you are ready to learn how to select the best one for your specific needs. In this guide, we provide step-by-step instructions on how to select the right level of outside support. We invite you to save, download, or print this guide and use it as a customizable worksheet for your business.

Step 1: Prioritize

Prioritize your systems and data. What are the most important ones for your business? What are your “crown jewels?” List them below.

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________
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. If this is the case, we encourage you to complete the Cyber Readiness Program and Cyber Leader Certification Program, and then reassess your needs.
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.

For more information on types of support organizations, professional credentials that help indicate an individual is knowledgeable, and types of organizations you may encounter, please revisit the second guide in this series: “Introduction to the Types of Outside IT and Cybersecurity Support.”

<table>
<thead>
<tr>
<th>Managed Service Provider (MSP)</th>
<th>Virtual CISO (vCISO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th><strong>MSP</strong></th>
<th><strong>vCISO (Information Security Advisor)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Setting up a network in a facility</td>
<td>□ Evaluating/comparing offerings from MSPs</td>
</tr>
<tr>
<td>□ Setting up a network in an office</td>
<td>□ Creating an incident response plan</td>
</tr>
<tr>
<td>□ Setting up a remote network</td>
<td>□ Monitoring access, firewall, and other logs and responding to anomalies</td>
</tr>
<tr>
<td>□ Setting up computers for new users</td>
<td>□ Tracking attack attempts</td>
</tr>
<tr>
<td>□ Setting up email accounts</td>
<td>□ Conducting network penetration tests</td>
</tr>
<tr>
<td>□ Installing and maintaining endpoint detection and response (antivirus) software</td>
<td>□ Establishing acceptable use of personal devices</td>
</tr>
<tr>
<td>□ Performing data backups</td>
<td>□ Establishing password and other standards</td>
</tr>
<tr>
<td>□ Testing backups</td>
<td>□ Ensuring systems are getting patched quickly and properly</td>
</tr>
<tr>
<td>□ Establishing multifactor authentication</td>
<td>□ Defining technical requirements and specifications, such as for VPN, firewall, other security safeguards (controls), network architecture, and/or cloud services</td>
</tr>
<tr>
<td>□ Setting up a VPN</td>
<td>□ Conducting vendor risk review</td>
</tr>
<tr>
<td>□ Installing and maintaining/patching software</td>
<td>□ Ensuring that computers are non-addressable from outside the network</td>
</tr>
<tr>
<td>□ Defining/implementing cloud services</td>
<td>□ Supporting company management in shaping culture</td>
</tr>
<tr>
<td>□ Providing help desk support</td>
<td>□ Defining security implications of cloud service vendors, provide standards</td>
</tr>
<tr>
<td>□ Implementing firewalls based on your network architecture</td>
<td>□ Defining and implementing methods to control access to systems and information so that authorized users have access to what they need and no more</td>
</tr>
<tr>
<td>□ Determining relevant data privacy regulations (e.g., GDPR, CCPA)</td>
<td>□ Aligning controls to meet relevant data privacy regulations</td>
</tr>
</tbody>
</table>

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.

The purpose of this guide is to help you determine how to select the right level of support. If you’re now faced with potentially confusing contracts, look for our next guide in this series, “Reviewing and Understanding the Contract.”
The complete list of guides in this series:

- Should I Get Outside Support to Manage My Cybersecurity Risk?
- Introduction to the Types of Outside IT and Cybersecurity Support
- Reviewing and Understanding the Contract
- Your Ongoing Cybersecurity Responsibilities
- How to Select the Right Level of Outside Support

Contributing Authors

- Marc Pillon, IT Ally
- Brian Kelly, EDUCAUSE
- Dawn Yankeelov, TALK
- Faye Francy, Auto-ISAC
- Ilene Klein, Cybercrime Support Network
- Jill Tokuda, CyberHawaii
- John Bryk, DNG-ISAC
- Michael Pritchard, Netchex
- Tanya Bolden, AIAG
- Walter Bran, ICC Guatemala
- Stan Stahl, SecureTheVillage

Special Thanks

About CRI

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). Explore the building blocks of good cybersecurity with our Starter Kit or create a cyber readiness culture in your organization with the self-guided, online Cyber Readiness Program. Our Remote Work Resources and Hybrid Workplace Guides offer timely tips for addressing the evolving cyber challenges of today. To find out more, visit www.BeCyberReady.com.