CYBER READINESS
INSTITUTE

Managing the Relationship with Your Outside Cybersecurity Provider

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

In the previous guide, we reviewed what you should look for in a contract with your outside support firm. Here we provide guidance on how to successfully manage the relationship. 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 IT support firm or managed service provider (MSP) 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 firm 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 the firm.

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. Use the check-in call to educate yourself about what they are doing for your company and new trends in technology and cybersecurity. Ask them if there are things you should be doing to reduce cyber risk and how they are continuously helping to reduce your cyber risk. Remember though, ultimately you are responsible for the human behavior in your company. By establishing a regular review with 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.

- ✓ Review responsibilities – theirs and yours – to make sure both parties are doing what was agreed upon.
- ✓ Evaluate your vendor through a survey on an annual basis. Consider evaluating on a bi-annual or quarterly basis depending on the criticality of the software.
- ✓ Request current information on service utilization (i.e., number of helpdesk tickets, number of accounts set up, date of last security vulnerability scan, number of open/missing critical updates, date of last phishing defense test and staff failure rate, date and status of last incident response test, remote access management, utilization of multifactor authentication, etc.)

The relationship you have with your outside support is one of the most important relationships for your company. We hope that this series 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 SMBs from CRI's Advisory Council

- No question is too small.
- Be proactive.
- Have a clear sequence of contact points to establish a line of communication at the service provider and validate that your provider knows who to contact within your business. Also, establish multiple contact points in case your main vendor contact is out of office.
- Check in frequently and set expectations.
- Take suggestions of what your business may be missing, especially considering other client relationships the vendor has.
- Your vendor should anticipate your needs and understand them such that they can assist before you know you need their assistance.
- Understand one another's values to establish trust. Make personal connections in the relationship.
- Constant communication is key. Build trust by engaging in back-and-forth communication, even if you don't have physical proximity or locality.
- Be clear on customer and provider responsibility boundaries. A customer always has a role in cybersecurity.
- Don't be befuddled with technical language. If you don't understand something the MSP is telling you, ask them to explain it in a less-technical way.

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

How to Select the Right Level of Outside Support

Reviewing and Understanding the Contract

Managing the Relationship with your Outside Cybersecurity Provider

(THIS GUIDE)

Contributing Authors

Special Thanks

- 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
- Lisa McAuley, Global Trade Professionals Alliance
- Srinath Sogal, Cyber Academy for Kids through Empowerment
- Kathy Schultz, SUNY Cobleskill
- Sean Filipowski, SUNY Cobleskill
- Pam Hurt, NCMS
- Michael Fillios, IT Ally
- Lee Ann Lyle, TALK

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.