CYBER READINESS
INSTITUTE

Understanding Your Cybersecurity Vendor Contract

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

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 and some tips on how to evaluate them. In this guide, we provide insight into what you (and/or your lawyer) should look in the contract. Beyond its legal aspects, the contract is a critical document in defining exactly what services will be provided and your ongoing responsibilities for cybersecurity.

We suggest you use the contract as a checklist to make sure that you and your service vendor have a mutual understanding of responsibilities going forward. You will want to make sure all of your expectations are addressed. Don't fall into the trap of waiting until there is a breach to understand what is covered in a contract and realizing it does not cover what you need.

It is important that you develop a trusted relationship with your service vendor. Ideally, the vendor will become part of the team helping your organization build and maintain a functional and secure IT capability. Making sure that you understand the contract and vendor responsibilities are critical to establishing trust from the beginning. Also, we suggest you have a quarterly audit with the service vendor during which you use the contract as a checklist to assess the relationship and how it is serving your company and its needs. Cybersecurity threats evolve rapidly, and you want to make sure you and your service vendor are not only responding, but proactively implementing measures to stay protected and be resilient.

We have broken this guide up into three parts: **Pre-Contract Review, Contract Checklist, and Guidance on Reviewing the Contract.**

info@cyberreadinessinstitute.com

Pre-Contract Review

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

Questions for Your Vendor

1. Identify your point(s) of contact at the vendor for specific services and who will be your ongoing relationship manager.
2. Check that vendor employees have had appropriate security checks (i.e., background checks) for handling proprietary information.
3. Confirm that your vendor has cyber insurance and verify the extent/limit of coverage in the event of a cyber incident at your company. This will help you identify possible gaps in coverage between the vendor's insurance and the insurance that you may or may not have.
4. Ask about their level of security controls and whether they are aligned with any standards or frameworks (certifications or credentials such as NIST 800-53, NIST Cybersecurity Framework, ISO27001, FedRamp, and/or audit reports, like a SOC2).
5. Understand the hours of service support (i.e., is it typical business hours or 24/7?) What is the vendor's availability "after hours"?
6. If they are hosting any software or data, understand where it is hosted and who controls those servers – and ask vendors to notify you of any changes. In some cases, the vendor may only be providing support to you and not hosting any of your software or data.
7. Determine if the vendor is using other services from other companies or subcontractors to provide the service to you.
8. Ask if the vendor is part of any organization or service that would provide threat intelligence.

Contract Check List

Below we provide some guidance on evaluating the contract you have with your cybersecurity vendor. In the following table, we offer some suggestions on the mandatory services that should be specified in the contract, along with some optional elements you should consider.

Mandatory

- ☐ Help Desk Availability – available support hours included in basic pricing package
- ☐ Documentation and User Guides for Relevant Hardware and Software
- ☐ Hardware Set-up (i.e., servers, laptops, wi-fi, smart phones)
- ☐ Software Installation and Updates
- ☐ Network Technical Support
- ☐ Consulting (virtual CIO)
- ☐ Backup and Recovery (scope, testing, frequency)
  - **Are the backups offline?**
  - **Are the backups encrypted?**
- ☐ Data Encryption Practices
  - **Is data at rest encrypted?**
  - **Is data in transit encrypted?**
- ☐ Priority Response Level Definition (examples below)
  - **PRIORITY 1 – enterprise wide – with immediate financial impact – less than 30 minutes**
  - **PRIORITY 2 – department or application specific problems – 30 minutes to 4 hours**
  - **PRIORITY 3 – impacted one person – 4 to 8 hours**
- ☐ Escalation Clause with Vendor for Unresolved Problems
- ☐ Primary Incident Response Contacts (vendor and customer)
- ☐ Minimum Security Controls Expectations
  - **Active Directory or equivalent set-up for access control**
  - **Network configuration**
  - **Timing of updates (e.g., vendor will patch critical vulnerabilities in 1 – 3 business days)**
  - **Vendor to notify if there is a security breach within set timeframe**
  - **Hosting and uptime target that includes a maximum targeted downtime**
  - **Visibility into where data is hosted**
  - **Onboarding process and timetable**
- ☐ Performance Termination Clause

Optional

- ☐ Network and System Architect/Admin
- ☐ Consulting Services (not elsewhere specified) and Sharing Industry Best Practices
- ☐ User Support for Remote Workers
- ☐ User Support for Employees Using Personal Devices
- ☐ After Hours Support
- ☐ Buying Power (hardware and software discounts through volume purchasing)
- ☐ Checking Logs (frequency)
- ☐ Frequency and Scope of Network Activity Reporting
- ☐ Participation in Conducting Cyber Response Exercises, Including Incident Response and Simulation Training
- ☐ Training (type and frequency, such as multi-factor authentication, VPN, secure data transfer, etc.)
- ☐ Assistance in Developing an Incident Response Plan
  - **Responsibility and roles in an incident**
  - **Additional costs associated with an incident**

info@cyberreadinessinstitute.com

Guidance on Reviewing the Contract

Some issues are negotiable, but you should ensure that you know what you are looking for in a vendor and have identified the correct type of vendor before you engage in a formal contract. If you need help selecting the right type of vendor, please revisit the **previous guides** in this series.

Below is a sample excerpt from a contract that outlines one vendor's overall approach to the relationship and the service they will provide. Not all service vendors will supply this much detail about their approach, but you can use this as a guideline for some of the general elements that should be addressed:

"Our team and Support Center also performs network management as well as acting as a focal point for all vendor contract management needs. **Additionally, we provide a skilled team, the infrastructure, and the resources for web and software design and development for projects such as database-driven web sites**. [MSP] provides a pro-active, personalized approach to problem resolution. [MSP]'s mission includes providing a professional, customer friendly environment for **onsite system administration and support** We achieve our mission through the right combination of people, processes and technology. Our approach enables us to deliver the highest levels of customer care, through our onsite staff and remotely through our Support Center. **We deploy quality technologies and customized documentation with specific business rules**, **workflows and device/ accessory/rate plan catalogues, to allow technology to implement policy**. Other Services offered: [MSP] provides alternatives to large **workstation and server troubleshooting** and support, **wireless devices**, information assurance, **data encryption**, **firewall prevention protection**, secure IT connections, biometrics, IT project management, **call center**, IT resource and support control, **Web surveillance**."

On the following page is an excerpt with specific contractual provisions. Note the level of detail about the timing of services and the specificity around client responsibility:

EXHIBIT A STATEMENT OF WORK No. S1-2017-205-433

Subject to the terms of the Professional Services Agreement ("Agreement"), the Parties enter into this Statement of Work ("SOW").

Termination

1. Period of Performance: The Initial Period of Performance will be November 1, 2018 through November 30, 2019. Unless a Party provides a written notice of termination prior to the end of the Initial Period of Performance, the Agreement will continue on a month-to-month basis until a Party provides written notice of termination in accordance with the Agreement.

Standard Help Desk Hours

2. Services: The Services will be performed on-site or remotely, as determined in [MSP]'s sole discretion, primarily at Client's location. Standard support will be provided between the hours of 9:00am through 6:00pm Eastern, Monday through Friday, excluding public holidays observed by the Client. After-hours emergency support and network monitoring will be provided 24/7/365.

Speed of Service

3. 2.1 Services Covered 2.1.1. **Help Desk:** [MSP] will provide a ticketing system (ConnectWise) and a **Remote Monitoring Management** (RMM) tool (N-able) as well as anti-virus (Sophos). Client will submit all issues through online client portal, email, or via hotline. Client will be able to receive email, phone, or remote support to help resolve any computer issues that may delay productivity. **In the event of an onsite emergency, an [MSP] technician will acknowledge within 30 minutes and begin travel onsite within 2 hours.** Any non-emergency onsite maintenance will be scheduled between [MSP] and Client but may be requested of [MSP] to be **performed within 4 business hours should Client determine it to be necessary to ensure IT operations.** [MSP] will respond onsite to any Client facility in the [city] area and travel will NOT be assessed as an additional cost. [MSP] will manage Client's email by providing end user management by adding or subtracting email accounts, user profiles, and computer setup. Client must provide 5 business days' notice prior to new user set up or user removal. Client will fill out template in Client portal provided by [MSP] for new users and termination of users."

This guide was designed to help you review and understand potential contracts before becoming formally involved with a vendor. In our next and final guide in this series, we will discuss how to manage the ongoing relationship once you have signed the contract. Remember, the purpose of the contract is to set expectations for building a trusted relationship between you and your service vendor.

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

(THIS GUIDE)

Your Ongoing Cybersecurity Responsibilities

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

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.