How to Manage Your MSP (Managed Service Provider) for Cybersecurity and Other Critical Services

Key Highlights

- Managed Service Providers (MSPs) are external third-party companies that provide various services. Managed Security Service Providers (MSSPs) specialize in security services.
- MSPs are important vendors for cooperatives, to provide an array of services when co-ops do not have the resources to do the tasks themselves, including cybersecurity.
- It is important for cooperatives to practice due diligence in selecting MSPs, and to conduct regular cybersecurity checks with the MSPs' operations and systems.
- NRECA's RC3 Legal Guidebook and other RC3 resources offer valuable recommendations for contracting with MSPs.
- NRECA's Self-Assessment Resources (online and hardcopy) can and should be referenced to identify maturity posture along with potential gaps in your environment. Keep this in mind as you read the advisory.

Introduction

A Managed Service Provider[1] or MSP is an external company (i.e., third party) that you contract with to provide various services. Basically, it is a company you can hire to do all the things your co-op does not have the time or resources to do yourselves. You can outsource almost anything to an MSP, from system backups to full IT support.

Types of MSPs

An IT MSP may provide system administration, manage email servers, and perform backups. An IT MSP may or may not provide cybersecurity services.

A Managed Security Service Provider (MSSP) specializes in security services. For example, an MSSP may help detect and defend against cyber-attacks and handle incident response.

MSPs and MSSPs are often confused, and rightfully so. Some MSPs may provide security in addition to IT, but still identify themselves as an MSP. It is important to understand what services you are paying for in hiring a third-party. In addition, many MSPs or MSSPs may subcontract or outsource some work to

[1] https://www.gartner.com/en/information-technology/glossary/msp-management-service-provider

other companies. In order to accurately manage risk, it is imperative to understand what work is contracted out, and how and when that work is utilized.

Contracts, SLAs, and MOUs

MSPs are valuable vendors for a co-op. It is important to apply the basics of vendor management when it comes to these MSPs, but also realize that circumstances may require additional diligence both before and during the term of the services being provided.

First, an electric cooperative should evaluate the pros and cons before outsourcing important business needs to an MSP, especially when it comes to information technology and security. The pros and cons will differ based on each electric cooperative's circumstances, but some general considerations are noted in the NRECA RC3 Legal Guidebook.

If you decided to outsource a business need, which MSP is best? Don't forget basic due diligence when determining which MSP to go with for your cooperative's needs. Remember that any vendor, not just an MSP, is a potential vector for cybersecurity threats. So, apply the appropriate degree of due diligence you would with any other vendor before you do business with an MSP. That would include asking MSPs to provide verifiable information to establish their reputation and ability to deliver. That process may include, but is not limited to, asking the MSP:

NRECA Rural Cooperative Cybersecurity Capabilities (RC3) Resources for Members

NRECA's *Rural Cooperative Cybersecurity Capabilities* (RC3) Program offers a variety of tools and resources to assist cooperatives in advancing their cybersecurity posture. One resource referenced repeatedly through this advisory is the RC3 Guidebook for Electric Cooperative Attorneys (also referred to as the RC3 Legal Guidebook). It is one in a series of guidebooks focused on the cybersecurity responsibilities of select job functions within a cooperative. For this and other cybersecurity resources, visit the RC3 website on cooperative.com:

www.cooperative.com/RC3

- What are its documented security policies and procedures?
- Are those policies and procedures tested and certified by an independent third party?
- Does it have a history of data breaches or cyber incidents? If so, what mitigation efforts has the MSP taken since?

The NRECA RC3 Legal Guidebook has an expanded discussion on vendor due diligence, including a sample questionnaire. In addition, a more extensive list of questions cooperatives may want to consider asking their MSP is provided in the Appendix at the end of this advisory.

Once your electric cooperative selects an MSP, the terms of the agreement – typically called a Service Level Agreement (SLA) or a Memorandum of Understanding (MOU) – are important for mitigating and shifting risk. Some cooperatives may not have enough bargaining power with certain vendors to negotiate favorable terms, which makes the due diligence discussed above even more important. Some of the key terms should focus on defining the scope of access to the co-op and its systems, testing of equipment and software before and after it is deployed, background checks for vendor's employees, standards for security controls, and rights to audit the MSP. Additionally, more traditional contract terms

NRECA America's Electric Cooperatives

to shift risk are equally important, like the MSP contractually agreeing to insure and indemnify the co-op against any risk of loss due to the MSPs negligence or failures to deliver as agreed. There is more on what contract terms to consider when contracting with an MSP in the NRECA RC3 Legal Guidebook. Electric cooperatives are encouraged to work with their attorneys when reviewing and negotiating contract terms with MSPs.

Finally, remember that no amount of due diligence or well negotiated contract terms are a guarantee to protect against all cybersecurity threats. However, due diligence, good agreements and vigilance can help mitigate the risk. What is important is to act reasonable under the circumstances, stay vigilant throughout the term of the agreement with the MSP, and exercise good judgment.

Tactical Measures to Take Upon Hiring an MSP

The following tactical actions should be taken immediately as precautionary measures if you are using an MSP:

- Ensure all unused accounts in your environment are disabled, and create processes to ensure accounts made for the MSP are unique, secure, and are disabled when MSP personnel change.
- Enforce multifactor authentication and log all vendors coming into your cooperative environment.
- Monitor for unexplained failed logins.

The Criticality of Testing and Backups

Many cybersecurity services are not used until something bad happens. Effective backups to cooperative system information are essential to quick and complete recovery after an incident. Backups should be done regularly and also at the time of any system upgrades. Your MSP may handle your system backups, but if you never test restoring those backups, they may not work. Finding out your backups are invalid after you have been hit by a ransomware attack adds insult to injury. Continuous security updates, configuration changes, and system upgrades should all invalidate confidence in previous test results. It is essential to periodically test each component of your incident response, business continuity, and disaster recovery procedures. It is recommended that back-up testing occur at least quarterly and upon significant changes to your system, such as large software upgrades, permission changes, etc. If you outsource critical functions to an MSP, involved them in your testing.

The Value of Exercises

Participating in external exercises or conducting your own is a good way to evaluate the effectiveness of your incident response, business continuity, and disaster recovery procedures. Tabletop exercises give everyone an opportunity to practice procedures and gain an outside view of potential threats, and are an excellent opportunity to uncover weaknesses or gain confidence in training, procedures, and system configurations. Annual or semi-annual exercises may be sufficient, if there have not been any major changes to your operating environment. Consider additional exercises and testing after major system upgrades or configuration changes. NRECA's RC3 program offers a series of Tabletop Exercises for members to use.

Additional Resources

DHS CISA has published several documents about MSPs, including:

- Risk Considerations for MSP Customers
- Mitigation and Hardening Guidance for MSPs, Small, and Medium-Sized Businesses

Additionally, in 2018 NRECA worked with APPA to produce a comprehensive list of MSPs.

For more cybersecurity information and resources, see NRECA's RC3 website on cooperative.com.

Contact for Questions

NRECA Rural Cooperative Cybersecurity Capabilities (RC3) Team at: *CybersecurityRC3@nreca.coop*

- Emma Stewart, NRECA Chief Scientist
- Ryan Newlon, Principal - Cybersecurity Solutions
- Justin Luebbert, Principal – Cybersecurity Compliance Solutions

NRECA
America's Electric Cooperatives

APPENDIX

Questions to Consider When Using an MSP

The following are some recommended questions for cooperatives to consider for due diligence prior to hiring an MSP. This is not an exhaustive list and cooperatives are advised to work with their legal staff to modify this list to meet their own individual needs.

Selecting Vendors

1. Are you vetting vendors by reviewing their security ratings or asking if they perform background checks on their employees?

Contracts and Agreements

2. Are there contracts in place? Has it been confirmed that the contracts have been read in their entirety by all essential staff? Have they been reviewed recently to ensure adequate familiarity?
3. Do contracts identify ownership of security roles and responsibilities?
4. Do your vendors have mature defined cybersecurity programs and policies in place that meet your organization's requirements? Examples include enforcing 2FA, performing regular penetration testing, providing employee cybersecurity training, along with incorporating cybersecurity best practices into their organizations' policies.

Starting with a New Vendor

5. Do you have an onboarding and offboarding procedure for vendors? Are you disabling vendors accounts not in use or that may no longer be needed?

Vendor Access to Co-op Systems

6. Are you using least privilege user permissions for vendors that access our environment to limit access and decrease threat surface?
7. Are you using individual accounts for each vendor that are not shared and have unique passwords for each account?
8. Are you logging and monitoring vendor access to your environment? How long do you retain logs?
9. Does the vendor have any connections in your environment that gives direct access to equipment? Do they have local login accounts, or do you ensure they are centrally managed via Domain and default passwords have been changed?
10. Have you set policies on the firewall to limit access to specific networks for the vendors?

Change in Vendor Personnel

11. Does the vendor have a formal process to regularly review access? How do they handle terminations and account disablement?

NRECA
America's Electric Cooperatives

12. Does the vendor have contractual obligation to identify when personnel with access to your site are terminated? Are adequate access revocation procedures in place?

Vendor Work

13. Are you reviewing and monitoring the vendors work and access?
14. Are you up to date on updates and patches, or if the MSP is providing that service, is there reporting and onboarding processes in place to ensure all assets are being patched in a timely manner?
15. How often are security patches applied in the vendors environment? Do they have a patching policy?
16. Do you have proper backups or, if the MSP is providing that service, do they have master backups and immutable backups to help protect against things like ransomware?
17. Do you have a proper response and recovery plan in place? Do you test it and how often? Do you engage with the MSP or vendor to review plans or conduct tabletop exercises?
18. Are you verifying vendors notification process and tools are working and alerting appropriately?

NRECA
America's Electric Cooperatives