Minnesota Counties Intergovernmental Trust
MCIT Resource
100 Empire Drive, Suite 100, St. Paul, MN 55103-1885 • 651.209.6400 • 866.547.6516 • MCIT.org

10 Cybersecurity Considerations When Contracting for IT Services

A local government may find that using skilled and trusted third-party information technology (IT) professionals and services for the organization can provide significant efficiencies and expertise without adding to headcount.

Contracting for technology services is not a way to eliminate harm that can be caused from a cybersecurity standpoint. Having technically trained professionals with eyes on the organization's technology stack can be excellent insulation from cyber threats. However, an arrangement for such services brings its own complexities that must be managed along with in-house data security measures.

To help ensure that the public entity's data remains secure, it should establish written contracts with all individuals or companies that access, collect, maintain, manipulate or store member data in any format.

It is critical that the contractual agreement is well-crafted from the start to manage risks and eliminate ambiguity in the event of a data compromise or cyber event.

The below 10 cybersecurity considerations when contracting for IT services focus on those areas that pertain to data and network risk management. A contract with a managed service provider (MSP) should also include provisions that address other areas of business management, such as the vendor's service hours, its pricing and the like.

What Is a Managed Service Provider?

Managed service providers (MSPs) are often instrumental in setting up new technology and keeping existing programs and devices online. MSPs:

- Offer a variety of services, such as for networks, applications, infrastructure and security.
- May provide (or not) ongoing regular support and active administration on a customer's premises, the MSP's data center (hosting) or in a third-party data center (cloud).
- Could offer their own proprietary services and/or other providers' services.

Typically, the level of service provided depends on the service agreement.

MSPs are not employees of the entity even though they may feel like it, particularly if they are on-site often or co-located with the public entity. Members need to remember that MCIT coverage does not extend to MSPs or other third-party contractors.

1. Conduct Due Diligence on Potential Vendor

The member should evaluate the MSP's data and cybersecurity measures before deciding to enter into a contractual service arrangement.

Private or nonpublic data and information is likely to be visible to technology vendors. The member ensures that internal staff are acutely aware of and trained on data protection requirements and the appropriateness of use when it comes to sensitive information.

Likewise, the member must take steps to verify that the MSP's systems are adequate to maintain and safeguard the security of this data. This would include understanding the service provider's password protocols, ways it secures pathways in and out of the member's systems, its use of multifactor authentication and encryption, and its security policies and procedures.

In short, the MSP should provide details about how it physically, technically and administratively controls access to and use of the member's private and nonpublic data.

To do this, the member may want to have the MSP complete a due diligence questionnaire. Standardized questionnaires are available from several sources that can be modified to meet the member's needs. Also, the Cybersecurity Self-assessment can be used as a starting point for a due diligence questionnaire.

If the MSP passes the due diligence test, then the member can move on to negotiating provisions of the contract for service. The agreement should explicitly detail important points of how the professional relationship will work for both parties.

2. Include Insurance, Indemnification Provisions

The contract with a managed service provider should include provisions that protect the member in the event that the MSP is negligent and causes harm to the member. These provisions include hold harmless and indemnification language, as well as insurance requirements.

MSPs may try to cap their damages or limit their liability in the agreement to the amount of, or some multiple of, the fee paid under the contract. This may be significantly inadequate to cover a potential loss.

Just as a contract for an electrician should make the member whole if the electrician's work sparks a fire that damages the facility beyond the cost of the contracted services, the agreement with an MSP should include hold harmless and indemnification provisions where the MSP is held responsible for its negligent acts, including covering the costs of attorney fees and breach notification costs, among other costs and expenses incurred due to the negligence.

The MSP should carry adequate bonding and insurance coverage to ensure that the service provider can cover costs of potential negligent acts.

3. Understand Business Continuity Plans

The agreement with an MSP should require that the service provider has business continuity and redundancy resilience to safeguard against any potential gaps in service or support should the vendor have an abrupt or unexpected change in its business.

The MSP should provide the member with a copy of its business continuity plan. If it does not provide a plan, this is a red flag, and the member should be wary of the vendor's reliability and ability to bounce back from an incident.

The MSP should also provide the member with its disaster recovery test results regularly. This allows the member to confirm that the service provider's recovery capabilities are actually sufficient.

4. Establish Scope of Service

Setting the professional expectation is paramount when initiating a contract for service. Ensure that the scope of service is clearly outlined and includes dispute resolution language in the agreement.

- Provisions should detail exactly what services the MSP is providing in exchange for the fee.
- Keep in mind that if a service is not noted in the agreement, the MSP is likely not obligated to provide it.
- If the agreement does not include data security services for the member, then the member is left to address that aspect of its IT risks independent of the MSP.

For example, when purchasing set up of a network from an MSP, the agreement may not include ongoing troubleshooting for the system or cybersecurity services. If the member needs these services, the agreement needs to account for them.

5. Detail Security Implications, Obligations

The agreement with an MSP should describe how the product or service implicates information security. What, if any, connectivity is necessary to the member's system? The details in this area help determine that risks are addressed elsewhere in the contract, such as the necessary insurance requirements.

Data Practices Requirements

If an MSP has access to sensitive databases, computer programs and the like, the member needs to establish and call out the obligations the vendor has to maintaining the privacy, confidentiality and security of that government data, such as adherence to the Minnesota Government Data Practices Act (MGDPA), Health Insurance Portability and Accountability Act and so on.

If the MSP is contracted to perform any of the government entity's functions, it is subject to the requirements of the MGDPA. The Act requires that the contract terms make it clear that all data created, collected, received, stored, used, maintained or disseminated by the private service provider in performing the government functions is subject to the MGDPA's requirements and that the private service provider must comply with those requirements as if it were a government entity.

Additionally, unless otherwise excluded by law, the MGDPA requires that in any contract where the government entity discloses government data on individuals to the MSP, the MSP must administer and maintain that data on individuals in accordance with the Act.

Members should not agree to confidentiality provisions that exceed the provisions of the Minnesota Government Data Practices Act.

Cyber-, Physical Access Security Provisions

Contracts should include provisions regarding both cyber- and physical-access security, particularly if vendors bring electronic devices or equipment and log in to any of the organization's systems. The infamous 2013 hack of retailer Target and its customers came from a breach of Target's heating, ventilation and air conditioning vendor.

Data security requirements may also include:

- Requirement to provide a written information security program that reasonably and appropriately engages physical, technical and administrative safeguards to:
  - Ensure the confidentiality, integrity and availability of member data stored within or transmitted to or from the MSP's systems.
  - Protect against reasonably anticipated threats or hazards to security or integrity of member data or services; and unauthorized access to, uses of or disclosures of member data.
  - Ensure compliance with all applicable laws by the MSP, its officers, employees, contractors, etc.
- Meeting minimum security measures as established by law or a reputable agency, such as the National Institute of Standards and Technology (NIST).
- Electronically transferring data classified as private or not public only when encrypted.

6. Review Performance Regularly

To ensure that the MSP is meeting its security obligations, the member may want to include provisions that allow it to monitor the vendor's obligations. This may include access to:

- Compliance certifications.
- Assessment of how faithfully the MSP has reported all known material breaches of security, fraud and other irregularities.
- The MSP's corporate ethics and social responsibility policies.

7. Termination Procedures

In the event that a member may need to terminate a business relationship with an MSP, it is best to have the termination steps and obligations called out before the relationship even starts. The termination plan should be sufficiently detailed to prevent disputes.

The MSP likely will have access to the member's critical data and services, so if the working relationship abruptly changes, clearly outlined obligations in the agreement will become critical to maintaining the member's normal business functions during a transition or termination of services.

At a minimum, the MSP should be obligated to assist with the transmission of data or transition to another vendor. Furthermore, ensuring that a past vendor no longer has access to data and information once its services are no longer needed is critically important to meeting the member's data security obligations.

The member may also need to include provisions for when and how the vendor should securely destroy the member's data that the MSP has in its systems.

8. Set Expectations in Event of Cyber Incident

MCIT members are obligated to notify MCIT immediately in the event of a suspected or confirmed data compromise or cyber incident to comply with coverage conditions. If the member contracts for IT services, the member is still the responsible party for notifying MCIT of an incident, not the MSP.

Similarly, starting in December, members are required to report cybersecurity incidents to Minnesota IT Services.* This includes when a government contractor or vendor that provides services to the member has a cybersecurity incident if the incident affects the member.

The MSP contract should outline how the service provider will notify the member if it discovers an issue and the timelines required for that notification. Best practice is to require the MSP to notify the member immediately upon discovery.

The member should consider requesting a written security plan from the MSP that details the steps the vendor takes in the event of a breach.

Require Cooperation

Beyond the need for immediate reporting, the member and MCIT need consistent cooperation from any outside technology vendors in the event of a data compromise or cyber incident. This may mean cooperation with an investigation, and plans for communicating with the public or procedures for notifying victims, for example.

In the case of a data breach or cyber incident, MCIT works toward a resolution with the member and MCIT's forensic and legal expert partners. The MSP may not be included in certain conversations to preserve attorney-client privilege. The MSP likely will not be part of decision-making on how to proceed toward a resolution of an incident. However, it may be engaged to help execute a plan.

That expectation of cooperation with MCIT in the event of a cyber incident should be included in the terms of the agreement.

9. Other Considerations for MSP Agreements

Define Terms

Most contracts include a section defining key terms related to the agreement. This is important so that the member and the vendor agree on what terms mean going forward in the contract and then in the working relationship.

For example, terms that may need to be defined, among others, are:

- Private data
- Nonpublic data
- Cyber incident
- Security incident
- Data breach

Software, Hardware Purchasing

If the organization intends to have an MSP involved in software or hardware procurement, the service contract should spell out how these agreements and renewals will be managed.

When the member maintains the ownership and contract duration of various hardware and software programs directly rather than an MSP, the member has greater control of the procurement process and eliminates potential entanglements in the event that the member may need to separate from the managed service provider.

MSP's Access to Data

Restrict the MSP's access only to data necessary to complete the scope of provided services. In doing so, the member limits the points of vulnerability to its systems and data, and thus, the potential for a cyber incident or data compromise.

10. Seek Legal, Risk Management Advice

Contracting for IT services can involve complex issues. Prior to signing a new, renewed or modified agreement with an MSP, members should have the contract reviewed by appropriate legal counsel and risk management personnel. Their change recommendations should be implemented so as to protect the organization.

Remember that each agreement for services will require an individual review and language specific to the facts and circumstances of that agreement. The language used in one section of a contract may not apply to or be sufficient for the same section in an agreement for a different IT service, for instance.

MCIT members can contact MCIT with risk management questions about an agreement or for additional information about best practices in this area.

* *See* Minn. Stat. § 16E.36; 2024 Minn. Laws Ch. 123, art. 17, § 24.