IT Security
Supply Chain
OT Security
Insider Threat
Physical Security
Interoperable Communications

CISA INSIGHTS

DEFEND TODAY,
SECURE TOMORROW

2 September 2021

Risk Considerations for Managed Service Provider Customers

Overview

To aid organizations in making informed Information Technology (IT) service decisions, the National Risk Management Center (NRMC) at the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed this set of risk considerations for Managed Service Provider customers. This framework compiles information from CISA and IT and Communications Sector partners to provide organizations with a resource to make risk-informed decisions as they determine the best solution for their unique needs. Specifically, **the framework provides organizations with considerations to incorporate into their IT management planning and best practices as well as tools to reduce overall risk.**

IT services enable business operations but can also be a complex, costly, and time-consuming enterprise for many organizations to manage on their own. Third-party vendors such as Managed Service Providers (MSPs) offer services that can reduce costs and play a critical role supporting efficient IT operations for organizations of all sizes. Many small and medium-sized businesses use MSPs to remotely manage IT systems, data, and applications. Nonetheless, outsourcing the management of networks, cloud infrastructure, applications, devices, and other IT elements to MSPs does not absolve an organization from risk management responsibilities associated with the IT enterprise. In some cases, by introducing third-party attack surfaces, partnering with an MSP can introduce unanticipated risks to an organization; therefore, organizations must weigh the benefits (cost, efficiency, capability) against potential risks when outsourcing IT services. If the decision is to outsource, it is critical that organizations proactively manage their cybersecurity risk and collaborate with their MSPs to jointly reduce that risk.

This framework is designed for government and private sector organizations of all sizes, and divides guidance into three audiences based on the risk calculations most often made by employees in these roles: (1) senior executives and boards of directors (strategic decision-making); (2) procurement professionals (operational decision-making); and (3) network administrators, systems administrators, and front-line cybersecurity staff (tactical decision-making). These categories are fluid and likely differ among organizations. Stakeholders should adapt the content of this framework to best fit their organizational structure. This framework complements and builds upon additional guidance from CISA on how MSPs and small- and mid-sized businesses contracting with MSPs can better mitigate against risk and harden their networks.[2]

Nation-State Threats to MSPs and Clients

Organizations have increasingly turned to IT service management providers in recent years. Nation-state affiliated Advanced Persistent Threat (APT) actors have historically targeted IT service providers by actively exploiting trusted relationships and network access granted to IT managed services vendors. APT groups try to steal data, disrupt operations, or destroy infrastructure by using sophisticated, long-term, and multi-staged attacks.[1]

[1] Cybersecurity and Infrastructure Security Agency, "APTs Targeting IT Service Provider Customers."
[2] Cybersecurity and Infrastructure Security Agency, "Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses."

Strategic Decision-Making

Senior executives must balance cost effectiveness and efficiency with reliability and security when considering whether to outsource IT services to an MSP. Outsourcing IT services does not absolve executives of risk management responsibilities. In order to balance these priorities, executives must maintain awareness of the technologies and systems supporting their operations. Executives must also understand the risks from potential loss of core organizational systems and services, loss of confidentiality, integrity, and availability of data, loss of consumer and market confidence, loss of productivity due to operational disruption, and fines, legal fees, or other regulatory costs, and other adverse financial impacts. Organizations must also account for risks to the vendors themselves, as vendors' financial health and other attributes can serve as indicators of potential future service disruptions.

CONSIDERATIONS AND BEST PRACTICES FOR SENIOR EXECUTIVES AND DIRECTORS

Who should have input on the decision of whether to outsource IT services to an MSP?

All organizational components or business units should provide input on their IT requirements and inform leadership decision on whether to outsource IT management to an MSP. In its "Key Practices in Cyber Supply Chain Risk Management" report, the National Institute of Standards and Technology (NIST) recommends companies establish a supply chain risk council that includes executives from across the organization and represents all relevant business units and organizational functions (legal, privacy, etc.).[3]

Is outsourcing cost-effective when accounting for security requirements and organizational risk thresholds?

The Chief Financial Officer (CFO), Chief Operations Officer (COO), Chief Information Officer (CIO), Chief Information Security Officer (CISO), and procurement officials should provide input to a cost-benefit analysis that weighs efficiencies from outsourcing against enterprise risks. Organizations without the technical expertise to fully assess those risks could hire an independent consultant to provide that analysis.

Who is responsible for security and operations when outsourcing IT services to an MSP?

The specific balance of responsibilities between a customer and a vendor will depend on several factors and should be jointly agreed to by customers and vendors after a careful consideration of associated risks and tradeoffs. Organizations share in the responsibility for faults or failures that impact business operations and affect customers. In order to minimize such disruptions when outsourcing IT services, organizations can define roles and responsibilities in a vendor agreement using the Shared Responsibility Model[4], which articulates the vendor's responsibilities, the customer's responsibilities, and any responsibilities shared by both parties. This model can serve as a framework for decisions, such as which entity applies patches, maintains hardware, or trains employees. Executives can also define a shared responsibility model that aligns with the organization's risk tolerance. Ceding more responsibility to an MSP may increase cost-efficiency but could also increase risk exposure. As vendors access networks and data, the potential cyber-attack surface increases and the organization's level of vulnerability may increase as potential vulnerabilities in the vendors' networks are compounded with any unresolved vulnerabilities on the organization's systems. Organizations may also lose visibility across their IT enterprise that could inform threat detection.

What are the most critical assets that we must protect and how do we protect them?

Organizations should develop and maintain an enterprise cybersecurity risk management plan that includes security, legal, and procurement priorities and accounts for risks from IT services provided by an MSP. Risk management plans should include an inventory of organizational assets and the degree to which each type of information or communications technology asset is exposed to risk. When possible, organizations should prioritize the protection of assets according to criticality of the threat posed and the importance of the asset to the organization.

[3] NIST, "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry," February 2021.
[4] Amazon Web Services, "Shared Responsibility Model."

Risk frameworks such as the NIST Framework for Improving Critical Infrastructure Cybersecurity and the Factor Analysis of Information Risk (FAIR) Cyber Risk Framework offer scalable, systematic approaches to identifying which assets need protection and calculating potential losses.[5,6] The FAIR Cyber Risk Framework also aligns with The Open Group Architecture Framework (TOGAF), which provides a baseline framework for designing, planning, implementing, and governing enterprise information technology architecture.[7]

To build resilience against potential incidents, organizations can:

- Develop, maintain, and exercise incident response plans, including senior leadership playbooks
- Hold regular cybersecurity threat briefings for C-suite executives and the Board of Directors
- Provide cybersecurity incident reporting, including mitigation and lessons learned analysis, to C-suite executives and the Board of Directors
- Develop risk-based key performance indicators to quantify cyber risk, measure program effectiveness, and compare with peer groups

Strategic Priorities for Small and Medium-sized Businesses

Small and medium-sized businesses (SMBs) may not have the financial resources or technical expertise to develop and maintain a comprehensive enterprise risk management plan but will nonetheless face risk management decisions when weighing whether to outsource IT services to an MSP.[8]

SMBs should catalog which assets are the most critical to operations and characterize the risk to those assets. This allows organizations to prioritize which assets should be included in or excluded from vendor agreements and to develop specific contingency plans for incidents affecting those assets.

SMB owners can then weigh risk management decisions by determining the following factors in potential vendor agreements:

- Which tasks and responsibilities will the MSP take on?
- Which will the SMB continue to execute?
- Which tasks and responsibilities will be shared?

Operational Decision-Making

Coordinated procurement, operations, continuity, and security requirements will decrease enterprise supply chain risk and improve system performance. Organizations with separate staff dedicated to each of those functions should coordinate IT requirements across organizational silos. For smaller organizations or those without staff dedicated specifically to these functions, an enterprise risk management plan should account for each of these requirements as part of an integrated approach to risk management at whatever scale is appropriate for the organization.

PROCUREMENT CONSIDERATIONS AND BEST PRACTICES

How does an organization account for the requirements of Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Operations Officers (COOs), Continuity Managers, and Chief Risk Officers when selecting a vendor?

A requirements management process that coordinates across functional areas will drive performance, reliability, and security.[9] Those in procurement roles should solicit a list of requirements from managers within the company whose departments use the IT managed services being considered at the beginning of the procurement process and maintain a requirements master list to provide a baseline for procurement decisions. In addition to the functional and performance requirements needed for the managed services, the list should also include specific

[5] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," April 2018.
[6] Fair Institute
[7] The Open Group Architecture Framework (TOGAF)
[8] Arnold, Robert. *Cybersecurity: A Business Solution.* 2017.
[9] The TOGAF Architecture Development Method (ADM) provides a useful framework for requirements management processes,

considerations for security, operational continuity, and other core business functions. It may be necessary to deconflict or clarify requirements between organizational components when finalizing and maintaining the requirements master list. The CIO, CISO, and representatives from each organizational component can validate whether a potential vendor can meet the organization's requirements. NIST recommends using a master requirements list and service-level agreement to formalize requirements with vendors.[10]

Organizations can use several methods to vet potential MSPs. For instance, the CISA and NIST joint publication, "Defending Against Software Supply Chain Attacks" includes best practices for preventing and mitigating risks in the software supply chain.[11] Additionally, the CISA Information and Communications Technology Supply Chain Risk Management Task Force published a Vendor Supply Chain Risk Management Template that offers standardized questions that foster clear and consistent communication between vendors and customers regarding security requirements.[12] Organizations can also require self-attestations from MSPs to validate the use of industry standards and best practices, maintained by continuous monitoring processes and tools.

What should an MSP provide to an organization in advance of contract award?

In addition to clearly articulating requirements in a contract and developing a Shared Responsibility Model to define roles and responsibilities, organizations should strive to solicit the following elements from any potential MSP prior to signing a contract:

- Specific performance-related service level agreements, including a clear delineation of operational IT services and security services
- Confirmation that the individual signing for the MSP is responsible for the product's security or service and a requirement to notify the customer of any change of MSP ownership or leadership and internal MSP measures to ensure the security of the organization's data
- Detailed guidelines for incident management, including the MSP's incident response responsibilities, warranty information, compensation for service outages, and plan to provide continuous support during a service outage
- Remediation acceptance criteria that define the steps the MSP will take to mitigate known risks
- A Software Bill of Materials (SBOM)[13] or similar verification of the security of any software the MSP will use to provide its services
- Statement from the MSP on how data from different clients will be segmented or separated on the MSP's networks
- Detailed guidelines for log and records maintenance, including requirements for the MSP to provide secure storage of backups and for detailed records of when accounts are accessed, by whom, for how long, and what actions were completed[14]
    - This should include physical access to storage, networking, and processing capabilities
- Documentation of vetting of employees (including subcontractors and independent consultants) to minimize risks of intellectual property theft, manipulations, or operational disruptions
- Direct access to security logging information, network intrusion detection, and anomaly analysis data telemetry from all systems managed by the MSP that support the service being procured
- The ability for the customer organization to examine the systems that directly and indirectly support the contracted service on-demand by the customer organization with appropriate data handling considerations

[10] NIST, "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry," February 2021.
[11] CISA and NIST, "Defending Against Software Supply Chain Attacks," April 2021.
[12] ICT Supply Chain Risk Management Task Force, "Vendor Supply Chain Risk Management (SCRM) Template," April 2021.
[13] National Telecommunications and Information Administration, United States Department of Commerce, "Software Bill of Materials."
[14] NIST, "Protecting Data from Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain and Test Backup Files."

- Transition plan to support a smooth integration of the IT services
  - Any required system downtime or outage to facilitate a transition should ideally occur at the time of the organization's choosing to minimize operational impacts
- Notification of any sub-contracts and independent consultants that would potentially expose the organization's data to another external party and documentation of the MSP's responsibility for any actions performed by subcontractors or independent consultants
- Protocol for planned network outages or other maintenance activities that could interrupt business operations
  - If possible, organizations should have input on the maintenance schedule to avoid or minimize any such disruptions
- Documentation of MSP's financial health, performance record for other clients, and disclosure of any previous legal issues

Executive Order 14028, "Improving the Nation's Cybersecurity," includes specific guidance on formulating contract language for IT and OT [operational technology] service providers supporting federal departments and agencies.[15] The guidelines in the Executive Order provide an additional resource for organizations to consider as they formulate contracts with MSPs. Organizations should also work with their counsel to conduct a legal review, as appropriate, of all MSP contracts.

Operational Priorities for Small and Medium-sized Businesses

Small and medium-sized business owners and executives may have multiple roles and associated responsibilities. Often roles like the CIO, CISO, and other C-Level roles do not formally exist, but the relevant functions are (or should be) managed at the executive level regardless of title.[16] However those responsibilities are assigned within an organization, establishing and enforcing procurement requirements, operational requirements, and security requirements will decrease risk, minimize disruptions, and improve organizational performance.

Specifically, SMBs should ensure that all parts of the organization (procurement, operations, security, etc.) weigh in on MSP requirements prior to contract award. The elements noted above and in the Vendor Supply Chain Risk Management Template provide a starting point, but SMBs should solicit input from across their organization to ensure their unique organizational requirements are accounted for in vendor agreements.

Tactical Decision-Making

Policies and controls on network access, controls, and logs, remain the organization's responsibility while outsourcing IT services to an MSP. Organizations should identify personnel responsible for monitoring and managing the day-to-day activity of MSPs and must set careful policies on the access given to any third-party vendors. Common examples of such policies include establishing clear requirements for authentication or verification and maintaining controls and logs separate from the vendor's records. Organizational policies and practices relating to the authentication of vendor logs and activities across the IT enterprise helps ensure appropriate and authorized activities by MSPs while protecting the client's interests from unauthorized activities.

CONSIDERATIONS AND BEST PRACTICES FOR NETWORK ADMINISTRATORS, SYSTEMS ADMINISTRATORS, AND CYBER DEFENSE PROFESSIONALS

What network and system access levels are appropriate for third-party service providers?

Organizations should apply the principles of the Zero Trust security model to their networks, including implementation of the Principle of Least Privilege to any MSP or affiliated sub-contractor and assign only the minimum necessary rights for the shortest necessary duration.[17,18] The specific access requirements will depend

[15] Executive Order 14028, "Improving the Nation's Cybersecurity," May 2021.
[16] Arnold, Robert. *Cybersecurity: A Business Solution*. 2017.
[17] National Security Agency, "Embracing a Zero Trust Security Model," February 2021.
[18] NIST CSRC glossary definition for principle of least privilege.

on the nature and scope of services the vendor is providing and will change over time. Organizations should regularly re-evaluate access requirements. When possible, organizations should define the vendor's required privilege and access levels prior to contract award to ensure vendors can meet service requirements under those security protocols.

CISA provided tactical guidance[19] for customers of MSPs to mitigate against risks from outsourcing to MSPs and harden their systems against nation-state Advanced Persistent Threat and cybercriminal activity targeting MSP customers:

- Manage supply chain risks
  - Understand the supply chain risks associated with your MSP, such as network security expectations
  - Manage risk across your security, legal, and procurement groups
  - Use risk assessments to identify and prioritize allocation of resources and cyber investment
- Implement strong operational controls
  - Create a baseline for system and network behavior to detect future anomalies; continuously monitor network devices' security information and event management appliance alerts
  - Regularly update software and operating systems
  - Integrate system log files—and network monitoring data from MSP infrastructure and systems—into customer intrusion detection and security monitoring systems for independent correlation, aggregation, and detection
  - Employ a backup solution that automatically and continuously backs up critical data and system configurations. Store backups in an easily retrievable location that is air-gapped from the organizational network
  - Require multi-factor authentication (MFA) for accessing your systems whenever possible
- Manage architecture risks
  - Review and verify all connections between customer systems, service provider systems, and other client enclaves
  - Use a dedicated Virtual Private Network (VPN) to connect to MSP infrastructure; all network traffic from the MSP should only traverse this dedicated secure connection
- Manage authentication, authorization, and accounting procedure risks
  - Adhere to best practices for password and permission management
  - Ensure MSP accounts are not assigned to administrator groups and restrict those accounts to only systems they manage. Grant access and admin permissions based on need-to-know and least privilege
  - Verify service provider accounts are being used for appropriate purposes and are disabled when not actively being used
- Review contractual relationships with all service providers. Ensure contracts include:
  - Security controls the customer deems appropriate
  - Appropriate monitoring and logging of provider-managed customer systems
  - Appropriate monitoring of the service provider's presence, activities, and connections to the customer network
  - Notification of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative networks
- Implement CISA's Cyber Essentials to reduce your organization's cyber risks

[19] Cybersecurity and Infrastructure Security Agency, "Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses."

What backups or records should an organization maintain?

Organizations should maintain their own offsite backups of essential records and network activity logs to facilitate recovery from a critical incident with an MSP. Backups and logs also allow an organization to authenticate vendor activity. For smaller organizations or those without sufficient technical expertise, a neutral third-party consultant may be necessary to facilitate incident forensics using network logs.

How should organizations incorporate vendors in incident response and business continuity planning?

NIST recommends organizations include key vendors such as MSPs in an organizations' incident response, business continuity, and other contingency planning, including in the organization's training on such plans. Organizations must update these plans regularly to align with changes in vendor relationships. NIST also recommends organizations and vendors establish clear protocols for vulnerability disclosure, incident notification, and communication with any external stakeholders during an incident. Organizations and vendors should also establish clear authorization protocols for threat hunting and incident response procedures on customer networks. Organizations should require that vendors provide timely and detailed reporting on incidents affecting vendor networks, even those that did not directly affect customer data and services. Finally, NIST recommends that organizations include vendors in after-action and lessons learned reporting.[20]

Tactical Priorities for Small and Medium-sized Businesses

SMBs outsource IT requirements to MSPs to achieve efficiency and cost-savings but cannot completely delegate IT responsibilities to vendors.[21] SMBs outsourcing IT services to an MSP should maintain full control of access to their systems and maintain awareness of vendor access by setting clear policies agreed to by the vendor. SMBs should also maintain logs of all MSP activity and have offsite backups of all critical data separate from the vendor's storage. These requirements should be included in vendor agreements and validated periodically.

Additional Resources

Information and Communications Technology Supply Chain Risk Management Task Force Resources

- Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists
- Vendor Supply Chain Risk Management Template

National Institute of Standards and Technology (NIST) Resources

- Cyber Supply Chain Management
- Risk Management Framework
- Cybersecurity Framework

[20] NIST, "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry," February 2021.
[21] Arnold, Robert. *Cybersecurity: A Business Solution*. 2017.

Appendix A: MSP Risk Considerations Checklist

TABLE 1: MSP RISK CONSIDERATIONS CHECKLIST

MSP RISK CONSIDERATIONS CHECKLIST

Considerations for Strategic Decision Makers

- □ Establish a supply chain risk council that includes executives from across the organization and represents all relevant business units and organizational functions (legal, privacy, etc.)
- □ Define roles and responsibilities in a vendor agreement using the Shared Responsibility Model to articulate the MSP's responsibilities, the customer's responsibilities, and any responsibilities shared by both parties
- □ Develop and maintain an enterprise cybersecurity risk management plan that includes security, legal, and procurement priorities as well as an IT services supply chain risk assessment
- □ Develop, maintain, and exercise incident response plans, including senior leadership playbooks
- □ Hold regular cybersecurity threat briefings for C-suite executives and the Board of Directors
- □ Provide cybersecurity incident reporting, including mitigation and lessons learned analysis, to C-suite executives and the Board of Directors

Considerations for Operators

- □ Solicit a list of requirements from departments who will use the services being considered and maintain a requirements master list
- □ Request the following from an MSP before signing a contract:
    - Specific performance-related service level agreements
    - Confirmation that the individual signing for the MSP is responsible for the product's security or service and a requirement to notify the customer of any change of MSP ownership or leadership
    - Detailed guidelines for incident management
    - Remediation acceptance criteria that define the steps the MSP will take to mitigate known risks
    - Statement from vendor on how data from different clients will be segmented or separated on the vendor's networks
    - Detailed guidelines for log and records maintenance
    - Documentation of vetting of employees to minimize risks of intellectual property theft, manipulations, or operational disruptions
    - Transition plan to support a smooth integration of the MSP's services
    - Notification of any sub-contracts that would potentially expose the organization's data to another external party
    - Protocol for planned network outages or other maintenance activities that could interrupt business operations
    - Documentation of MSP's financial health, performance record for other clients, and disclosure of any previous legal issues

Considerations for Tacticians

- □ Define the MSP's expected privilege and access levels prior to contract award
- □ Apply a Zero Trust security model, including the Principle of Least Privilege, to any MSP or affiliated sub-contractor and assign only the minimum necessary rights for the shortest necessary duration
- □ Review and verify connections between MSP and internal systems
- □ Restrict Virtual Private Network (VPN) traffic to and from an MSP to a dedicated VPN connection
- □ Implement strong operational controls, manage authentication, authorization, and accounting procedures, and ensure managed service providers' accounts are not assigned to administrator groups and restrict those accounts to only systems they manage
- □ Maintain offsite backups of essential records and network activity logs
- □ Validate logs of MSP activity on network and across the IT enterprise
- □ Include key suppliers in organizations' incident response, business continuity, and other contingency planning
- □ Establish clear protocols for vulnerability disclosure, incident notification, and communication with any external stakeholders during an incident
- □ Include the MSP in after-action and lessons learned reporting

For more information or to seek additional help, contact us at NRMC@hq.dhs.gov.