Supply Chain Risk Management

Your organization's security is only as strong as its weakest link – and that link could be your vendors. From LastPass to GoDaddy to MSP hacks and more, suppliers can leave you vulnerable to cyberattacks.

It's critical for every organization to establish and maintain **an effective supply chain risk management program** to assess and contain risks from interconnected services, including cloud vendors, software developers, hosting providers and non-technical suppliers. This includes fourth-and fifth- party risks that may be invisible until disaster strikes.

The NIST Cybersecurity framework includes five controls for managing supplier risks. At LMG, we've summarized these as follows:

- Develop Your Processes (ID.SC-1)
- Know Yourself and Your Suppliers
- Delegate Requirements Through Contracts
- Assess Supplier Risk
- Involve Suppliers in Incident Response Planning and Vetting

Use this handy checklist as a framework for maintaining an effective supplier risk management program.

✓ Develop Your Processes (ID.SC-1)

"Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders"

- Identify key stakeholders
- Assign roles and responsibilities
- Develop policies and procedures
- Establish security standards and requirements for your suppliers (make sure to include review of supplier's supply chain risk management)
- Develop a standard methodology for prioritizing and assessing suppliers
- Establish time frames for remediating any issues identified
- Implement a risk escalation procedure (for non-responsive or non-confirming suppliers)
- Maintain a process for vendor input and feedback
- Track current industry standards and resources for informing program development and revision
- Review/revise supplier risk management program on a regular basis

✓ Know Yourself and Your Suppliers (ID.SC-2)

"Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process" – NIST ID.SC-2

- Enumerate and track information resources

  - ○ Data mapping
  - ○ Asset management
  - ○ Cloud services
- Classify information resources based on confidentiality and availability needs
- Enumerate suppliers
- Minimize supplier access
- Prioritize suppliers based on access to confidential data, availability needs, etc.
- Routinely review list of suppliers, priorities and access

✓ **Delegate Requirements Through Contracts (ID.SC-3)**

"Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan."

- Establish standardized contractual obligations for suppliers
- Ensure that supplier agreements contain appropriate clauses
- Track any deviations from baseline contractual obligations and review periodically

✓ **Assess Supplier Risk (ID.SC-4)**

"Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations."

- Identify points of contact for each vendor with respect to cybersecurity risk management
- Communicate the process and schedule for reviewing and validating cybersecurity requirements
- Routinely assess suppliers and validate that cybersecurity requirements are met
- Track any non-confirming results
- Escalate non-remediated issues as appropriate

✓ **Involve Suppliers in Incident Response and Security Planning (ID.SC-5)**

"Response and recovery planning and testing are conducted with suppliers and third-party providers"

- Ensure that key supplier contacts are maintained in the IRP contacts and kept up-to-date
- Establish a single point of contact for suppliers to report incidents, and make sure suppliers are aware
- Hold proactive conversations with high-priority suppliers regarding incident response, including expectations for communication, evidence availability, and more
- Integrate suppliers into the incident response plan as appropriate
- Identify high-priority suppliers to include in interactive incident response activities, such as tabletop exercises