BAKER'S DOZEN
13 ELEMENTS OF AN EFFECTIVE SCRM PROGRAM

1. Obtain executive-level commitment to support a Cyber-Supply Chain Risk Management (C-SCRM) program.
2. Supply chain security is a team sport, collaborate throughout an organization—horizontally and vertically.
3. Conduct criticality assessments to identify, assess, and prioritize critical assets, systems, processes, and suppliers to guide C-SCRM.
4. Share threat, vulnerability, and consequence information to inform supply chain decisions across the enterprise.
5. Manage supply chain security as a primary metric, along with cost, schedule, and performance, when assessing a vendor's ability to meet contract requirements.
6. Conduct robust due diligence on suppliers and vendors associated with critical systems.
7. Include supply chain security requirements, including cyber breach and data breach notifications, into the terms of the contract with suppliers and vendors.
8. Monitor suppliers' adherence to agreed-upon SCRM-related security requirements.
9. Identify and protect sensitive business information about your organization and customers.
10. Establish reciprocal information sharing mechanisms and requirements with suppliers for threat and vulnerability information.
11. Manage C-SCRM risks when terminating relationships with third-party vendors.
12. Develop and implement workforce training on managing, mitigating, and responding to C-SCRM activities.
13. Establish plans and manpower/workforce requirements for contingency operations; exercise plans regularly, update as needed.

FORTIFY THE CHAIN