The Pitfalls of Supply Chain Risk Management

Também disponível em português
www.isaca.org/currentissue

Many organizations have progressively increased their reliance on a growing number of global suppliers. As evidenced by the numerous supply chain attacks over the past decade, such as the 2013 Target data breach[1] and the 2020 SolarWinds supply chain attack,[2] cybersecurity threat actors often target suppliers because they are less secure than larger organizations higher in the supply chain. These attacks compromise the software or products of the supplier organizations lower in the supply chain, allowing the compromised software or products to facilitate the infiltration of the larger organizations.

The increased reliance on large, global supply chains and the increased threats to them have moved supply chain risk management to the forefront of industry conversations on cybersecurity best practices. The need for supply chain risk management is no more important in this decade than in the last—it has simply become better recognized. In May 2021, the President of the United States issued an executive order directing US federal resources to fund guidance on supply chain security.[3] In addition, in 2021, the UK's National Cyber Security Centre conducted a survey on supply chain risk management.[4] Most survey respondents identified barriers to implementing an effective supply chain risk management program for their organizations. These barriers included poor visibility into supply chains, a lack of expertise in cybersecurity risk and insufficient tools or assurance mechanisms to evaluate supplier cyberrisk.

DAVID PODESWIK | CRISC

Is a cybersecurity risk and compliance analyst for a Fortune 1000 company. He leads the cybersecurity risk and compliance team and focuses on third-party risk management and regulatory compliance and cybersecurity policy.

Supply chain risk management programs can be beneficial to every organization, but without proper guidance, they can actually increase risk. Misguided supply chain risk management practices, such as the aggregation of audit or assessment artifacts, is lowering the effectiveness of these programs. In addition, the seemingly unending creation of unique cybersecurity questionnaires is contributing to increasing burdens that detract from suppliers spending time securing their organizations. The risk of these misguided supply chain risk management practices can be managed by acquirer organizations having their supply chain assessors review artifacts without having to collect and store them, smart sizing the level of the risk assessment to the risk the vendor poses to the acquirer organization and assessing risk with a commonly used risk management framework.

Taking Action

Many organizations are taking action against supply chain cyberrisk by establishing or improving their supply chain risk management programs and processes to better mitigate supply chain risk. The three most common assurance mechanisms used to validate supply chain security are similar to mechanisms used by assessors and auditors to validate US National Institute of Standards and Technology (NIST) controls. These methods, described in NIST Special Publication (SP) SP 800-171A *Assessing Security Requirements for Controlled Unclassified Information*[5] and NIST SP 800-53A Rev. 5 *Assessing Security and Privacy Controls in Information Systems and Organizations*,[6] are examine, interview and test. When applied to the supply chain, organizations should:

1. Examine artifacts such as documentation
2. Interview individuals or groups within the supply chain
3. Test controls to see if they behave as expected

These methods are frequently employed by a dedicated individual or team within the organization or a contracted third party.

Another consideration for organizations improving their supply chain risk management procedures is data privacy assessments. Depending on the external regulatory requirements and the organization's policies, the data collected as part of these assessments could require additional data privacy assessments. An example of a common data privacy assessment required by organizations is the EU General Data Protection Regulation (GDPR) Data Protection Impact Assessment (DPIA).[7] Although this regulation covers only a portion of data privacy transactions, these same concepts are emerging within many similar regulations globally. Depending on the information exchanged and the types of processing performed, privacy assessments may be required or just simply desired as a part of good information hygiene for organizations.

Paved With Good Intentions

As organizations choose the best methods for dealing with new threats, they are potentially opening their organizations and their supply chain to additional risk. Although the intent may be good, there are five misguided practices that often plague supply chain management efforts:

1. Aggregation of artifacts from multiple suppliers into one single location within an organization higher up in the supply chain creates risk.
2. Having suppliers with minimal knowledge of the acquirer organization's security measures protect artifacts (a nondisclosure agreement [NDA] alone does not guarantee the security of those artifacts) creates risk.
3. Shared artifacts expand the risk surface for suppliers and acquirers—often exponentially:
   - Each new organization that receives these artifacts increases the risk surface for each organization in business with the supplier.
   - As acquiring organizations gather documentation on their supply base, they are holding larger and larger stores of valuable security information.
4. Third-party vendors used to manage and store these artifacts expand the risk surface even further.
5. Organizations often have unique questionnaires and artifact requirements, which puts increased burden on the suppliers providing this information and detracts from the valuable time needed for the effort to improve the security of these suppliers.

Aggregating and Securing Artifacts

It has become more common for organizations to request documentation and artifacts from their supply chains that, if discovered by a threat actor, would be harmful to the supplier and the organizations receiving their products. **Figure 1** demonstrates examples of the proprietary artifacts that are often requested.

FIGURE 1
Examples of Artifacts Often Requested From Suppliers

Network diagrams	System baselines and security configurations	Methods of cryptographic key management
Incident response plans	Multifactor authentication (MFA) deployment locations	Patch management and patching report results
Business continuity plans	Email provider information	Endpoint security names, versions and capabilities
Disaster recovery plans	Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-Based Message Authentication Reporting and Conformance (DMARC) settings	Mobile device management (MDM) versions and capabilities
Vulnerability scan results	Data loss prevention (DLP) tools and rules	Locations and numbers of security personnel
Log management and security information and event management (SIEM) information	Asset inventory	

Based on the risk to the supplier and product, it is a good idea to validate these items and determine whether they fall within industry standards. However, collecting them without a specific course of action is an unnecessary risk to take. If a threat actor obtains these artifacts, it gives them a road map to help them breach the supplier.

Figure 2 illustrates the aggregation of artifacts by one acquirer across multiple suppliers. Although this figure shows only four suppliers, there can easily be hundreds or thousands of suppliers providing artifacts to one acquirer.

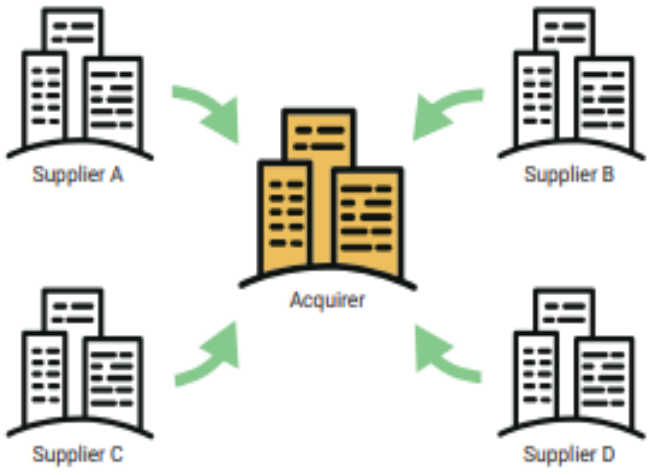
Aggregating supplier artifacts operates with the assumption that the acquiring organizations have impenetrable security, but no organization is unbreachable. Every time suppliers provide artifacts to acquiring organizations, they risk allowing proprietary information to be leaked in a breach. In addition, suppliers often have minimal knowledge of the acquiring organization's security posture, allowing these artifacts to be stored in an unknown location with unknown security.

Risk Surface Increase

Every acquiring organization that obtains these artifacts increases the risk surface of every other organization doing business with that supplier. Acquiring organizations often have a narrow-minded view that the supplier relationship is 1:1, but that is rarely the case. One supplier can supply hundreds or thousands of other organizations.

FIGURE 2

Aggregating Artifacts



As acquiring organizations continue to gather artifacts from suppliers, they create an ever-expanding store of critical security information that threat actors desire. If one organization with this treasure trove of data is breached, the security of their suppliers is compromised, and threat actors will have an advantage against all other organizations working with each of those suppliers.

"The landslide of numerous questionnaires, artifact requests and unique frameworks has put large burdens on suppliers."

Figure 3 illustrates the relationships that occur when a supplier begins to distribute their proprietary information to multiple acquirers. If each acquirer collects these artifacts, they all need to be aware of each other's involvement. Acquirer 1 is now reliant on acquirers 2, 3, 4 and 5 to protect this data from their supplier. This same reliance is true for each other acquirer. If acquirers 1, 2, 3 and 4 are all protecting the data securely, but acquirer 5 is breached, that information is no longer secure. Everyone in that supply chain is now at higher risk.

Third-Party Vendor Services

Cybersecurity is expensive and the skills gap for properly trained personnel is not closing anytime soon. This is pushing acquirer organizations to utilize third-party vendor services to manage this process. These third-party vendors can help interpret and review the risk of suppliers. However, if they are collecting artifacts in the same manner as the organization, it can make the problem worse. Third-party vendors may have worse security, keep copies of the artifacts and forward copies to the acquirer organization. This example puts those artifacts in three different places, with the supplier, the acquirer and the third-party vendor, which offers more opportunity for threat actors.

The Burden

The supply chain risk management process is necessary but can be burdensome if executed improperly. Often, acquirer organizations have positive intentions in improving their security posture, but they may not understand the best path forward for improvement. Determining the proper depth and

coverage for a risk assessment can be different for each organization and organizational relationship.

The landslide of numerous questionnaires, artifact requests and unique frameworks has put large burdens on suppliers. Many suppliers are now devoting significant security resources to answering questionnaires and providing artifacts to acquirers, diverting personnel from roles that can make positive changes to improve the security of the supplier organization. Organizations must consider the appropriate level of depth and coverage for the risk presented. Suppliers that provide higher levels of risk should be scrutinized more heavily, while those with lower levels of risk should be reviewed with less rigor.

Solution: Reduce the Risk Surface

Instead of addressing every supplier the same, acquirer organizations should consider categorizing their suppliers based on potential impact and addressing the risk management process in a tiered manner. **Figure 4** demonstrates an example hierarchy of ways to measure supply chain risk without aggregating artifacts. Within each risk review action, the assessor or auditor reviews the presented attestation or artifacts and documents their findings according to an organizationally determined risk framework.

For example, at the higher tiers of risk, the assessor or auditor can review the artifacts over an unrecorded video teleconference meeting or in an in-person visit. The results of the review can be documented in a minimally descriptive summary. In addition, it should be noted whether the supplier's controls ultimately meet each requirement or not. Because the artifacts will remain within the supplier's possession, artifact hashing can be used to ensure that the artifacts the assessor or auditor reviews can be reviewed again later. An example of this method is described further in the CMMC Artifact Hashing Tool User Guide.[8] These methods ensure the artifacts do not need to be moved off-premises and aggregated into a large repository. Organizations need to determine their own

"Instead of addressing every supplier the same, acquirer organizations should consider categorizing their suppliers based on potential impact and addressing the risk management process in a tiered manner."

FIGURE 3
Distributing Artifacts

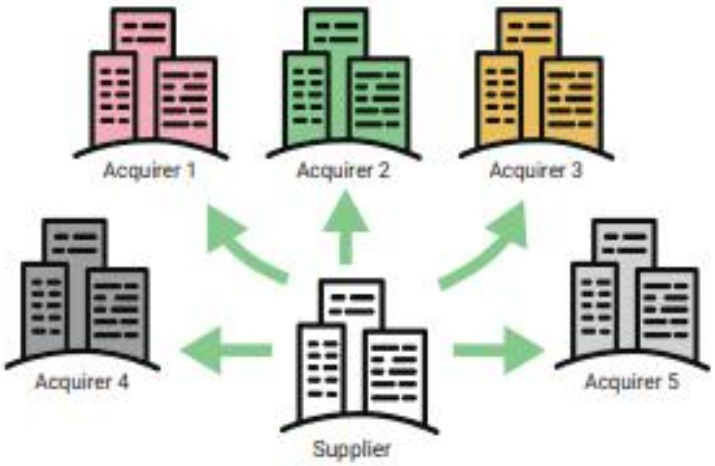


FIGURE 4
Example of Tiered Solutions Based on Potential Impact

Potential Vendor Impact Level	Risk Review Actions
Critical	In-person visit, artifact hashing
High	Unrecorded video teleconference
Medium	Supplier self-attestation aligning to a commonly used cybersecurity framework that maps to others (e.g., US National Institute of Technology [NIST] Special Publications [SP] 800-171A, NIST SP 800-53, International Organization for Standardization [ISO]/International Electrotechnical Commission [IEC] 27001, Cybersecurity Maturity Model Certification [CMMC])
Low	Basic supplier self-attestation aligning to a commonly used cybersecurity framework that maps to others (e.g., Federal Information Processing Standards [FIPS] Publication 200, NIST SP 800-171 basic security requirements, CMMC Level 1)

risk appetite for each level of potential impact and adjust their risk management strategy accordingly.

An alternate method that can help reduce the burden on suppliers and shrink the risk surface of artifact collection is the use of a shared evaluation platform, such as Exostar. "Exostar started out as a cooperative effort by BAE Systems, The Boeing Company, Lockheed Martin, Raytheon, and Rolls Royce."[9] These organizations have highly sensitive vendor relationships and had the foresight in 2000 to create a platform that allowed the aerospace and defense industry to properly manage their vendor relationships without burdening suppliers with unique questionnaires or aggregating unnecessary artifacts. Using guided methods such as these allows acquirer organizations to reduce their risk surface and position their risk management programs for success.

Solution: Protect Acquired Data

If acquirer organizations do obtain artifacts from suppliers, they should be protected according to industry cybersecurity standards. Some of the most important and easily missed protections include encryption, access controls, data retention periods and data sanitization.

Artifacts should not be kept indefinitely. There should be a data retention period assigned to those data. The usefulness of the data deteriorates over time, and once they are determined to be no longer useful, they should be sanitized according to commonly accepted sanitization methods, such as NIST SP 800-88 *Guidelines for Media Sanitization*.[10]

Conclusion

Cyber supply chain risk management is a practice that all organizations should be performing, but strategic implementation is imperative. If suppliers are burdened by limitless requirements and forced to give up artifacts, including proprietary documentation, acquirers may be unintentionally sabotaging their own security without realizing it. Based on risk, acquirer organizations should consider in-person visits, unrecorded video teleconferences or self-attestation from suppliers. In addition, the depth and coverage of assessments should be scaled to the level of risk. Supply chain risk management programs can be beneficial to all organizations, but without proper guidance, they can increase risk for organizations across the globe.

LOOKING FOR MORE?

- Read *Supply Chain Resilience and Continuity*. *www.isaca.org/supply-chain-continuity-2020*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Endnotes

1 United States Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach*, Majority Staff Report for Chairman Rockefeller, USA, 26 March 2014, *https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883*

2 US Department of Homeland Security, Emergency Directive 21-01, USA, 13 December 2020, *https://cyber.dhs.gov/ed/21-01/*

3 The White House, *Executive Order on Improving the Nation's Cybersecurity*, USA, 12 May 2021, *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*

4 Department for Digital, Culture, Media and Sport, *Government Response to the Call for Views on Supply Chain Cyber Security*, United Kingdom, 15 November 2021, *https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security/government-response-to-the-call-for-views-on-supply-chain-cyber-security*

5 Ross, R.; K. Dempsey; V. Pillitteri; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171A *Assessing Security Requirements for Controlled Unclassified Information*, USA, June 2018, *https://doi.org/10.6028/NIST.SP.800-171A*

6 National Institute of Standards and Technology (NIST), SP 800-53, Revision 5 *Security and Privacy Controls for Federal Information Systems and Organizations*, USA, September 2020, *https://doi.org/10.6028/NIST.SP.800-53r5*

7 European Commission, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5, 2016, *https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1*

8 Carnegie Mellon University, The Johns Hopkins University Applied Physics Laboratory LLC, Futures, Inc, *CMMC Artifact Hashing Tool User Guide, Version 2.0*, USA, December 2021, *https://www.acq.osd.mil/cmmc/docs/HashingGuide_V2.0_FINAL_20211203.pdf*

9 Exostar, LLC, *Exostar: The Supply Chain Partner for Aerospace and Defense*, 2017, *https://www.exostar.com/file/2017/06/SupplyChain_SolutionOverview_June2017.pdf*

10 Kissel, R.; A. Regenscheid; M. Scholl; K. Stine; NIST SP 800-88, Revision 1, *Guidelines for Media Sanitization*, USA, December 2014, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf*