Success Patterns for Supply Chain Security

John Pescatore
Supply chain threats are real, ongoing and increasing, and they have been impacting businesses across all three elements of the well-known confidentiality, integrity and availability (CIA) triad. There have been a number of recent high-visibility and costly supply chain incidents that demonstrate the importance of establishing or upgrading a supply chain security program:

- Attackers compromised installations of the Adobe Magneto e-commerce platform and other third-party services in more than 7,000 business applications, stealing passwords and sensitive user information from companies such as Ticketmaster.1

- Universal Music Group had internal servers compromised when a cloud data storage contractor exposed UMG’s internal FTP credentials.2

- IT outsourcer and consulting firm Wipro had its infrastructure compromised by a targeted phishing attack, putting all of its services’ customers at risk.3

- British Airways was hit with a $230 million GDPR fine after a data breach caused more than 380,000 user records to be compromised by malware installed at websites running third-party payment services.4

---

The Council of Supply Chain Management Professionals defines supply chain management as follows:

“Supply chain management encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third party service providers, and customers.”

As the definition points out, the supply chain consists of not only vendors—it also includes many different types of partners that might play multiple roles. Figure 1 shows the complex and multilayered nature of the typical supply chain.

Applying the CIA triad model of security, a straightforward definition of supply chain security is “assuring the confidentiality, integrity and availability of business products and services across the entire supply chain.”

While the definition is simple, delivering effective supply chain security services often requires major changes in security architectures and processes. Even organizations with mature security programs are often focused on protecting systems and information inside the business rather than including what is coming into and going out of the business. Delivering supply chain security requires some key changes in cybersecurity governance and operations:

• The CISO and the security program must communicate effectively with many more internal groups (procurement, marketing, legal, customer support, business units, etc.) and work to be more integrated into their processes.

• The heterogeneous and volatile nature of most supply chains dictates that supply chain security processes provide tiered levels of security assurance.

• Tools for assessing and monitoring supply chain security levels must have modes or views that support use by non-security and non-IT users, such as procurement teams and business unit managers.

---


6 Adapted from “Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP800-161.pdf](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP800-161.pdf), p. 8, Figure 1-4
Making these changes will often require backing from senior management because such changes in process will often require groups outside of the security group and outside of the company to make changes. Security teams could use the aforementioned examples to illustrate the reality and scope of the financial risks, but CEOs and boards of directors will want to see that strategies are in place and metrics have been established to demonstrate reduced levels of supply chain risk.

Supply Chain Security Standards and Guidelines

There have been three different time periods in which supply chain security has been addressed in the past 30 years:

- The focus on materials and subassembly quality in the 1970s and 1980s resulted in the ISO 9000 standards, and ISO 9001 applied those principles to supply chain management.
- The terrorist attacks against the US in September 2001 drove the development of physical supply chain security standards mainly focused on how terrorists might disrupt shipping and importing of goods or use those channels to deliver weapons of mass destruction.
- The growth of ecommerce, Internet-connected logistics and delivery systems and the use of cloud computing after 2010 was the impetus for the development of supply chain security guidelines that focused on cybersecurity risks and controls.

In addition to high-level security frameworks such as the NIST Cybersecurity Framework and ISO 27001/27002, the supply chain-specific standards that are most relevant today include:

- **ISO 20243**—In 2010, The Open Group, along with industry and government representatives, created the Open Trusted Technology Provider Standard as a recommended set of guidelines for assuring the integrity of IT-centric supply chains. It became an ISO standard in 2018.
- **NIST 800-161**—NIST Special Publication 800-161 provides guidance to government agencies for implementing a multi-tiered supply chain risk management approach that integrates with the overall Risk Management Framework.
- **ISO 27036**—This standard provides detailed guidance on the security controls in ISO 27001 and how they should be applied to business-to-business supplier relationships, including a section on cloud service providers.
- **ISO 28000:2007**—ISO 28000 is a standard for supply chain security management that is used as the basis for accreditation against many national trade/import/export/shipping security requirements. It is more applicable to the physical security side of the supply chain.

---

7 [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf)
9 [www.iso.org/standard/44641.html](http://www.iso.org/standard/44641.html)
The Council of Supply Chain Management Professionals lists “risk minimization” as one of its 10 best practices for supply chain programs:

“Risk mitigation goes hand-in-hand with policies and controls, and best-in-class supply chain organizations integrate risk-mitigation methodologies into their sourcing decision process.”

However, many organizations have only informal supply chain management programs, and even mature, best-in-class programs have blind spots and weak points when it comes to cybersecurity. Three key barriers drive the most common deficiencies:

- The security program is not included in the evaluation, selection and monitoring of supply chain partners, or
- The security program’s tools and processes for performing risk evaluation and mitigation of supply chain partners cannot operate at the speed of business needs or scale to the number of supply chain partners.
- The security team and the metrics it uses are often speaking a different “language” than the business unit and corporate managers.

The first barrier is a common obstacle to all areas of cybersecurity: In order to reduce overall risk, security needs to be integrated into all aspects of business. To be both effective and efficient, security programs must be part of procurement, hiring, operations, facilities, merger/acquisition and other business critical processes. CISOs and other security leaders need to have the communication and collaboration skills required to establish these relations. Often, the support of the CEO and/or board of directors is key for gaining the backing necessary to overcome organizational obstacles that stand in the way of integrating security into those processes.

However, to make those relationships succeed, the security program must have the processes, skills and tools to be able to operate at the speed and scale required by business operations. Supplier/partner risk assessments that take months to complete or monitoring approaches that many partners will be unable or unwilling to support will cause the supply chain loop to quickly bypass the security program—and often with upper-level management backing to do so, because the continual negative impact on business of the security program is seen as equal to or higher than the risk of a potential security incident!

Business supply chains are much more heterogeneous and volatile than the typical IT supply chain. IT groups work to minimize device, server, network equipment, software and cloud services vendors. While the IT group for a large company might have hundreds of suppliers, that same company will likely have thousands or tens of thousands of partners in the overall supply chain.

---

10 “10 best practices you should be doing now,” www.supplychainquarterly.com/topics/Procurement/scq201101bestpractices
11 “Influencing and Effectively Communicating to CEOs and Boards of Directors,” www.sans.org/webcasts/influencing-effectively-communicating-ceos-boards-directors-103927 [Registration required.]
Similarly, IT supplier decisions tend to happen on yearly schedules, driven by planned procurement cycles. While some business supply decisions have similar predictability, changing market and competitive landscapes that do not honor annual budgeting cycles drive many (if not most) decisions. Supply chain security processes need to support both planned and pop-up risk analysis and mitigation.

The “language” barrier is a common complaint of CEOs and boards: The security team too often doesn’t express risk in the same way that the COO, CFO or business line managers do. That doesn’t mean they expect the CISO to express every risk in financial terms such as ROI, but that the security program must show how potential supply chain risks could impact critical services that are enabling the business to meet financial and operational performance promises to shareholders and customers.

Common Supply Chain Security Program Patterns

To succeed, any effort to develop or enhance a supply chain security program needs to start with a realistic assessment of the current state of the organization’s approach to supply chain security and must define the needed outcome. One approach is to base the assessment on a maturity model approach, in which higher levels of security maturity are tied to business benefits. This is most effective if the organization is already using the maturity model approach for IT operations or the overall cybersecurity program.12

If the organization does not already use a maturity model, another approach is to look at common patterns of supply chain security effectiveness to define where the organization is now and how it could further progress toward a more effective and efficient approach (see Figure 2).

Let’s look at each of the common patterns of supply chain security programs:

- **Pattern 1: Greenfield (Starting from Scratch)—**
  Many enterprises (especially smaller ones) have no coherent supply chain management processes in place—even though their policy documents say such processes should be in place—and consequently have no formal processes for supply chain security. Other organizations may be using defined supply chain management approaches in procurement and other areas, but the security group has no involvement or integration. Any organization that finds itself here has nowhere to go but up toward supply chain security.

---

• **Pattern 2: Reactive (Hey, Look What We Noticed!)**—Security groups that are not integrated into the supply chain management process will often discover third-party risks as part of regular vulnerability scanning or periodic threat hunting and penetration testing. The organization may have evolved repeatable processes for notifying management of the newly discovered risk, but it is still operating in a purely reactive manner.

• **Pattern 3: Included in the Vendor Selection or Partner Integration Evaluation**—Most businesses have long recognized that allowing a business partner to directly connect to their network and systems is risky, and many security groups are involved in doing a risk assessment prior to allowing such connectivity. Some organizations have also evolved to include security criteria as part of the vendor evaluation criteria. However, today the rate and quantity of such requests often exceeds the security group’s ability to respond. All too often, once a partner is approved, the security group is no longer involved—continuous monitoring or evaluation is not part of the process.

• **Pattern 4: Continuous Risk Monitoring and Evaluation**—The security group is integrated into the front-end procurement decisions and processes, and tools are in place to detect and investigate (and ideally mitigate) increases in supplier risk. At this level, these processes can scale to the quantity and heterogeneity of the full supply chain, meaning the security group has the staffing for manual processes or uses tools to support scaling.

• **Pattern 5: “Pretty Good” Supply Chain Security Program**—Both business and threats never stand still; supply chain security programs can’t either. Security operations and supply chain security programs may be effective at dealing with known threats but perform poorly in the face of emerging threats that will quickly impact supply chain partners. Similarly, as a supply chain security program matures, “inner-loop” processes (such as the initial risk evaluation of suppliers or their recertification) need to be made more efficient, both in resource usage and the time required to perform.

• **Pattern 6: The Adaptive, Effective, Efficient Supply Chain Security Program**—A well-managed and integrated supply chain security program is one that cohesively integrates across the life cycle of the supply chain and across the business, with continuous monitoring and improvement. This is obviously the most effective and efficient approach to reducing the business impact of real-world threats to complex supply chains. This is also the level in all maturity models that very few organizations reach, but it defines the end goal that can drive intermediate steps and decisions in the right direction.

These patterns, ordered here from least to most mature, are common across industry and government. In a maturity model, the goal is always to move higher in maturity. However, operational decisions (in areas such as organization governance, risk tolerance, staffing constraints and outsourcing philosophies) play a strong role in the realities of supply chain management. Even if such factors dictate remaining in a certain pattern, there are many steps security groups can take to reduce risk.
Large organizations may have extensive vendor risk management and/or supply chain security programs with large staffs, detailed policies and processes that meet the definition of Pattern 4 but lack the ability to move quickly enough to keep up with changes in threats or the business demand for speed. Adding tiered levels of assessment processes and tools with views that work for non-security groups can close the gap. Some organizations might be able to react quickly in some areas but lack full coverage, and they need to focus on gaining visibility and response across the board.

Conversely, smaller security teams that have been stuck in greenfield or reactive patterns generally must first find champions in corporate management or in business units and look to external services for support. Making these relationships is key to enabling processes and tools to be integrated for effective visibility and rapid risk reduction. The following sections describe the key components and a hierarchical approach to making such improvements.

### Key Components of an Effective Supply Chain Security Program

There are a number of common features of successful supply chain security programs. The features are listed in order of priority, as illustrated in Figure 3.

Developing and implementing processes for all five functions will not be feasible or necessary for every business, but each ability provides the foundation for adding the functions that follow as demands and risk require.

#### Find a Friend

Security must have a champion in the management chain responsible for supply chain decisions (board, CEO, chief operating officer [COO], chief legal, head of procurement, CIO, etc.) to ensure that security is involved at some level above greenfield. This requires the CISO or security manager to first develop trust and credibility with management and then to collaborate with the aforementioned groups versus simply issue security dictates.

Because the majority of CISOs report to the CIO, the IT group is the logical starting place. Cloud service and SaaS providers are part of the supply chain, and IT also often uses managed services, consultants, in-sourcers and other partners that introduce risk, particularly intellectual property data leakage.
In many organizations, the COO or equivalent oversees most supply chain functions and should be the “find a friend” starting place. There may already be a supply chain management program in place that has not considered cybersecurity. If your COO briefs the board of directors, see if you can obtain a copy of the most recent presentation and find the areas where increased supply chain security aligns with the COO’s metrics, plans and strategy.

Similarly, if your organization has an ISO 9000 quality effort or equivalent, it often will include supplier quality controls and processes that can provide a logical home for supplier security considerations. In 2016, SANS gave Boeing’s Procurement Manager John Martin a SANS Difference Makers award for doing just that.13

Discover Suppliers

The Center for Internet Security Critical Security Controls14 has long pointed out that the foundation of any successful security programs starts with asset management, vulnerability assessment and configuration control: You can’t secure what you don’t know is there, and if you know it is there, you must be able to detect when risk status changes. The equivalent in supply chain security is portfolio management: discovery of all supply chain partners, from Tier 1 partners to extended networks of suppliers, regular assessment of vulnerabilities and detection of changes in exposure.

Having the security group formally integrated into key corporate processes is the starting point:

• Because most supply chain partners bill the company for their services, having security integrated into procurement processes will lead to early identification and assessment of supply chain partners.

• The chief legal counsel or equivalent is another integration point, as he/she usually reviews all corporate contracts and is often involved in compliance and auditing issues.

• The chief financial officer (CFO) may have responsibility for reviewing all business partners for financial risk and stability.

• Enterprise resource planning and logistics management systems (such as SAP and Oracle) may be in use to track all third-party services and can provide programmatic interfaces for supply chain partner discovery.

• Active Directory groups or VPN directories may have been established for third-party connections, providing an opportunity for automating the discovery of existing and new third-party connections and accounts. IT, network or security operations may also use discovery tools that will expose third-party connections. Network access control (NAC) tools that are often used to detect BYOD use on corporate networks will also detect and often profile third-party laptops or other devices in use by contractors on the local network. Cloud service monitoring tools will show the equivalent for SaaS usage by third parties.

There is no single, automated approach for accurate and up-to-date knowledge of existing supply chain partners. Almost all organizations will need to use a mix of these approaches.

13   www.sans.org/cyber-innovation-awards/year/2016
14   www.cisecurity.org/controls
Scale Multiple Assessment Approaches

A “one-size-fits-all” risk assessment approach will not work for most businesses. A mix of techniques, from rapid “first look” to detailed, in-depth assessments, is necessary to support business responsiveness demands and to enable more continuous monitoring of risk levels.

One of the common reasons that the security group is bypassed, both overall and in supply chain management, is that “security moves too slowly.” Often the demands of business require business managers to accept some increased level of risk because of the greater risk of being late to market. Supply chain security programs need to provide tiered levels of assessment to support business needs.

In order of lowest to highest level of assurance, consider using the following techniques:

- **Vendor self-assessment questionnaires**—Having vendors fill out questionnaires and/or attest to compliance with common standards is often necessary to satisfy legal counsel requirements and limit liability, but it is never a sufficient means for assessing supply chain partner risk. Updating and tracking questionnaire responses can often require more resources than the value provided.

- **External risk-rating services**—Procurement organizations have long used financial risk-rating firms such as Dun & Bradstreet as part of evaluating the viability of a supplier. More technically oriented risk-rating services have become available (called “Security Rating Services” by Gartner\(^\text{15}\) and “Cybersecurity Risk Rating Services” by Forrester\(^\text{16}\)) that look at externally visible indicators to provide numerical risk scores of companies.

- **Questionnaire exchanges or shared assessments**—Many organizations have implemented “questionnaire exchanges” to shared supplier ratings. Some industries (such as banking) have formal “shared assessment” programs, in which all members use a common questionnaire (such as Shared Assessments\(^\text{17}\)), and if one member does a detailed assessment of a supplier, all members can decide if they will accept the results. Differences between business models and processes, as well as different risk-tolerance levels, often require additional assessments to be performed. There are also voluntary benchmarking programs (such as the Building Security in Maturity Model\(^\text{18}\)).

- **Active testing**—For critical suppliers or ones that will be part of the supply chain for “crown jewel” critical business applications, active testing of a supply partner provides the most detailed insight, but it comes at the highest cost—and is often resisted by suppliers with many customers requesting the same level of testing.

An efficient and effective supply chain security program will require a mix of these capabilities (either internally or using external services) to support “fast path” initial risk assessments in time-critical cases, as well as deep-dive, thorough, active assessments when more time and budget are available.

---

\(^{15}\) [www.gartner.com/document/3884271](http://www.gartner.com/document/3884271) \[Registration required.\]

\(^{16}\) [www.forrester.com/report/The+Forrester+New+Wave+Cybersecurity+Risk+Rating+Solutions+Q4+2018/-/E-RES142874](http://www.forrester.com/report/The%20Forrester%20New%20Wave%20Cybersecurity%20Risk%20Rating%Solutions%20Q4%202018/-%2F%E-RES142874) \[Registration required.\]

\(^{17}\) [https://sharedassessments.org](https://sharedassessments.org)

\(^{18}\) [www.bsimm.com](http://www.bsimm.com)
Extend Dashboard/Reporting to BU and IT Managers

There is no such thing as a zero-risk supplier, and corporate or business unit management is ultimately responsible for accepting the residual risks that have been identified. Supply chain security processes and tools should provide visibility into current risk views to non-security personnel and enable them to incorporate risk information in their decision-making processes.

If your organization already uses some standard approach for rating the financial or viability risk of suppliers and partners, the supply chain security reporting and monitoring should ideally integrate into that. If no such system exists, the supply chain security reporting visual style or data should be as similar as possible to what procurement, logistics and business operation managers are familiar with: high/medium/low; red/yellow/green; A–F; FICO-like scores, etc. No matter what the scale is, trend reporting should always be provided.

Close the Loop

Years ago, the manufacturing industry learned that quality programs couldn’t succeed just by rejecting low-quality suppliers; they also had to close the loop to drive all suppliers to adopt higher-quality processes. An effective supply chain security program must include feedback to vendors and visibility into the results of assessments and ratings to remediate open issues and drive improvement overall.

Summary

As many companies have learned in the past few years, when attacks against supply chain partners succeed, the customer blames the business, not the supply chain. Just as most attacks directly against business can be avoided by reaching “basic security hygiene” levels, the same is true with supply chain security—with one critical added factor: Supply chain security processes need to incorporate flexibility to be able to operate at the same scale and speed at which procurement and partnering decisions are made. Organizations that have been able to develop, deploy and operate effective and efficient supply chain security programs use a mix of assessment and monitoring capabilities that include business unit and procurement decisions makers.

The keys to minimizing the risk of damage due to attacks on or through your supply chain are:

- Rapid discovery and continuous monitoring of supply chain connections and partners, as well as lower-tier providers they are using
- The use of processes and tools that operate at the speed and scale of the supply chain
- Integration of cybersecurity concerns early in the procurement evaluation and decision process
- Ability to provide non-security managers and operations personnel with timely, accurate and understandable supplier risk information

The good news is that supply chain security is high on the list of priorities for many boards of directors and many customers. By demonstrating a strategic approach to improving (or creating) your supply chain security program, security managers can gain support for the changes necessary to make meaningful and efficient increases in supply chain security.
John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and “the occasional ballistic armor installation.” John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

SANS would like to thank this paper’s sponsors:

INTEROS

Panorays
<table>
<thead>
<tr>
<th>Event Name</th>
<th>City, Country</th>
<th>Start Date</th>
<th>End Date</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oil &amp; Gas Cybersecurity Summit &amp; Training 2019</td>
<td>Houston, TXUS</td>
<td>Sep 16, 2019 - Sep 22, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Rome September 2019</td>
<td>Rome, IT</td>
<td>Sep 16, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Raleigh 2019</td>
<td>Raleigh, NCUS</td>
<td>Sep 16, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Bahrain September 2019</td>
<td>Manama, BH</td>
<td>Sep 21, 2019 - Sep 26, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Dallas Fall 2019</td>
<td>Dallas, TXUS</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS San Francisco Fall 2019</td>
<td>San Francisco, CAUS</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Kuwait September 2019</td>
<td>Salmiya, KW</td>
<td>Sep 28, 2019 - Oct 03, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Northern VA Fall - Reston 2019</td>
<td>Reston, VAUS</td>
<td>Sep 30, 2019 - Oct 05, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Cardiff September 2019</td>
<td>Cardiff, GB</td>
<td>Sep 30, 2019 - Oct 05, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Riyadh October 2019</td>
<td>Riyadh, SA</td>
<td>Oct 05, 2019 - Oct 10, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Doha October 2019</td>
<td>Doha, QA</td>
<td>Oct 12, 2019 - Oct 17, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Cairo October 2019</td>
<td>Cairo, EG</td>
<td>Oct 19, 2019 - Oct 24, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Santa Monica 2019</td>
<td>Santa Monica, CAUS</td>
<td>Oct 21, 2019 - Oct 26, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Orlando 2019</td>
<td>Orlando, FLUS</td>
<td>Oct 28, 2019 - Nov 02, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Houston 2019</td>
<td>Houston, TXUS</td>
<td>Oct 28, 2019 - Nov 02, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS Dubai September 2019</td>
<td>OnlineAE</td>
<td>Sep 14, 2019 - Sep 19, 2019</td>
<td>Live Event</td>
<td></td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
<td></td>
</tr>
</tbody>
</table>