International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V3I4P118
Eureka Vision Publication | Volume 3, Issue 4, 189-194, November - 2022

Original Article

3rd Party and Supply Chain Risk in Oil & Gas

Vilas Shewale
Independent Cybersecurity Researcher, USA.

Abstract - The oil and gas business relies on a long supply chain. Hardware and software that run the automation and digital capabilities are sourced from several hundred vendors and integrators. This runs the whole gamut from the control systems that run pipelines (SCADA) and refineries (DCS), the machinery that drives drilling (rig automation), that spins pipelines and other equipment (turbomachinery), that measures the quantities of gas or liquid in midstream storage, on to the software-based platforms that perform analytics in the cloud based on all that data. Since 2020, numerous supply chain security breaches-SolarWinds, Kaseya, Log4Shell and credential abuse patterns-have demonstrated that these external relationships are an attack vector. Why is oil and gas different from some other critical infrastructure? How have prominent cyber events stressed this industry and what guidance has arisen as a result? We provide a way forward by presenting a framework for a vendor risk program designed to cover five stages: identification of third-party relationships, tiering the suppliers by risk level, defining contract requirements with those vendors, onboard vetting procedures and ongoing monitoring of vendor activities. The content below deliberately generalizes to help oil and gas organizations apply the recommended vendor risk processes to any specific ecosystem of vendors and integrators they may have.

Keywords - Supply Chain Risk, Oil and Gas, Third-Party Risk, SBOM, ICS, Vendor Management, Critical Infrastructure.

1. Introduction

Whether the manager of a refinery operation, an upstream oil production site or a pipeline run is still the manager of a portfolio of suppliers. Those PLCs came from Vendor A. Vendor B provides the historian. Vendor C hosts the analytics platform. A system integrator hired a systems integrator, who hired another integration vendor and so on, eventually ending up at a third-party cloud provider, who provides the analytics tenancy. A security lens was not used to vet these vendor relationships, nor could they be so easily dissolved or worked around if it were a vulnerability or other issue within their business that were to hit home.

Supply chain risk in the Oil and Gas industry has become a first-order problem and needs to be the target of a long-term work plan, not just an audit of one-off purchases. First, I would note the 2020-2022 period saw disruptive failures in critical infrastructure that spread across company boundaries because a compromise was made at a third party. This has included such as an incident via managed service provider or a software vendor's update channel or an open-source component that was leveraged in production and used to introduce compromise [1][2][3]. Lastly, NIST has since then come out with the Cybersecurity Framework version 2.0 and specific implementation guides that have replaced far vaguer NIST guidance that was available a mere 3 years ago. NIST has joined ENISA and CISA in issuing guidance, none of which could be seen as coherent three years back [4][5]. Companies are having difficulty with how this has trickled down and resulted in ownership vacuums between procurement groups, as these teams are not generally conversant with how to think of their problems from a security-centric perspective, leaving programs stagnant because these do not readily cross between contract and operating sections.

What follows here consists of an overview of what distinguishes the oil and gas supply chain in section 2. Some illustrative recent events between 2020 and the date this paper is published appear in section 3, offering playbooks for operating firms based on key lessons from each incident. In section 4, we briefly discuss the frameworks available. A practical approach to managing vendor risks is sketched in section 5 and section 6 lists the aspects still facing obstacles. Each figure serves to portray an array than replacing textual descriptions.

2. Why Oil & Gas Faces a Distinctive Supply Chain

Three structural features make the sector’s supply chain unusual. Each shows up in incident postmortems and in the time, it takes operators to remediate after a vendor compromise.

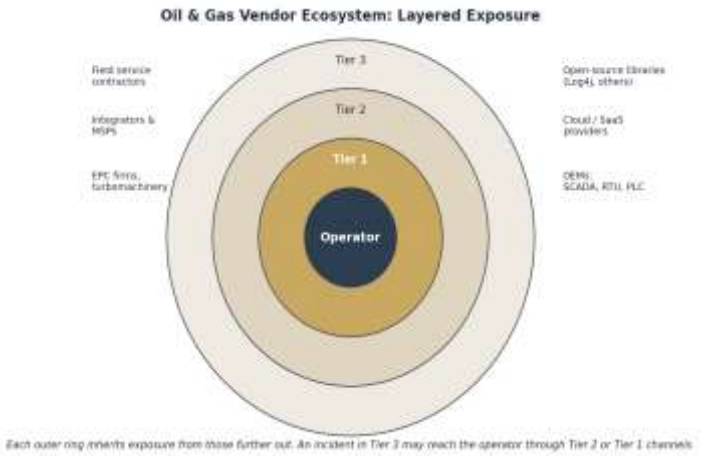


Figure 1. Oil and Gas Operators Inherit Risk through Layered Vendor Relationships. Each Outer Ring is harder to Inventory and Audit than the One below it

First, there are many vendors and many are clustered in odd areas. Some operators get 90% of their PLCs/controllers from a few OEMs but then depend on hundreds of smaller vendors for the parts, services and software that make up an industrial process. A historian's connector might be different from an analytics platform connector and each is different again from a custom driver for a temperature probe on an isolated platform or calibration software for pressure gauges. OEMs tend to be regularly audited, mature contractors with established agreements. The long tail is unkempt. Most operators do not know the names of all the vendors with logical access to their ICS systems, a fact that says a bit about where security practices have landed for a majority.

Second, ICS is an " install-it-and-forget-it" type of technology. Some of the equipment on a wellhead put in in 2007 will likely run for a couple of more decades. The firmware on it, the drivers, the engineering software-it all needs to stay current and secure over that period and the company that developed it might be on their third acquisition by the time they install a replacement unit. When the original vendor disappears or becomes absorbed into a different business, the onus shifts back onto the operator or whoever they can hire to figure it out.

Third, the oil &, gas industry is heavily reliant on contractors and integrators. Maintenance on pipelines, major turnaround projects, automation for the drilling process, operations on the control room-all are routinely outsourced to third-party service providers. Each comes in with their own laptops, accounts and in some cases, a custom network segment connected to the SCADA network, with varying degrees of vetting applied. Oil &, gas interfaces with vendors have historically been less regimented than in many industries, the industry prioritizes operational flex and control flow than security in favor of vendor access and integration at the earliest stages.

To make things worse, operations are geographically disbursed. There are often thousands of small facilities with no personnel onsite that need to be remotely accessed across a large footprint, even between countries. Drilling teams move rigs across different continents. Security teams cannot easily monitor all the points of vendor access from a central hub and typically, the local IT footprint is meager and is not a huge concern until some kind of major failure requires it.

3. Recent Events and What They Taught Us

Several incidents over the last three years shaped how operators think about supply chain risk in the industry. The point of recounting them is not to relitigate the technical details, which have been covered extensively elsewhere, but to extract the pattern.

3.1. SolarWinds, December 2020

SolarWinds Orion compromise showed how the software's build process at one company could be compromised and then used as a vector to deliver malware to many thousands of customers, many of whom were US government agencies and some of the world's largest companies [6]. The oil industry's exposure was initially limited since not many SCADA stacks contained Orion, but the implication was broader: even software signed by an established provider should no longer be trusted by default and the state of the supply chain is another attack vector, though one no more visible to the oil company operator than to the library creator itself.

Figure 2. Attack chain pattern in abstract. A vulnerability or other problem in a software library, build chain or signing stage is passed on via the legitimate supply chain down to the consuming systems.

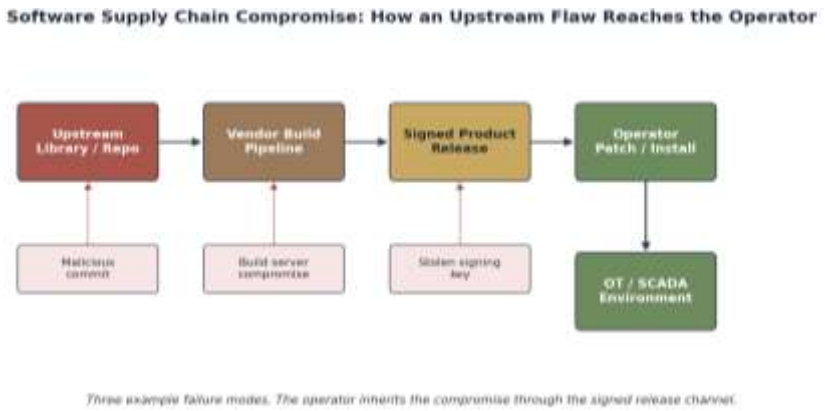


Figure 2. Three Example Failure Modes in The Software Supply Chain. The Compromise Reaches the Operator through the Legitimate Signed Release Channel

3.2. Kaseya, July 2021

An oil company got hacked by Kaseya MSP. To them it means they do not pay for Kaseya software and that MSP is responsible for the breach of their client, a petroleum company, which caused an outage for thousands of downstream organizations. [2] Not specific to Kaseya but MSPs were involved and a bunch of operators contract their MSP for patch/monitoring/endpoint services. MSPs hold privileged access to the clients, so the clients may have ransomware propagating into their systems within a couple of minutes.

3.3. Colonial Pipeline, May 2021

There are often mentions of ransomware about Colonial Pipeline, yet the supply chain facet deserves attention. Reports state the intrusion began when ransomware pirates used an account with legacy VPN credentials that did not support multifactor authentication, the login info somehow leaked through previous security compromises [7]. This obsolete account was operational technical debt left untouched. Leaked login data came from a separate security breach, the conjunction of the two triggered the worst critical infrastructure damage the United States had seen.

3.4. Log4Shell, December 2021

Log4Shell (the Log4j RCE issue discovered December 2021) put the concept of software bills of materials [3] to the test. Operators found Log4j in some of their industrial control software they did not associate with a Java logger-historian add-ons, vendor configs, analytics suites. Oil and gas were not special. The vulnerability impacted only as far as deep open-source dependencies went into the tech stack and what the operators know about it.

3.5. Incontroller / Pipedream, April 2022

A custom toolset that specifically targeted some of GE's and Siemens' products [8] has recently been discovered by CISA and its partner agencies. Although CISA was not aware of it ever being used in a live attack situation, the disclosure does tell us something interesting: that someone had put forth the effort and developed the tools to attack specific, oil-industry targeted products-the everyday tools that oil and gas operators run-at a granular level. While not an existential threat at present, this could lead to changes in supply chain processes. Specifically, operators are starting to pressure OEMs with much stricter requirements for securing their products, which are now focused on stronger authentication protocols, discouraging default credentials and a "secure by default" configuration mindset.

4. Frameworks and Guidance

I feel I am able to assist a great deal; the guidance landscape has really opened up. Nobody needs to go home and reinvent vendor risk from square zero. This has become more apparent through the publication of several significant guidance documents.

NIST SP 800-161 Revision 1 [4] Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (May 2022) is the most comprehensive treatment to date of supply chain risk management for information and communication technologies [4]. It provides specific guidance across enterprise-, mission- and operational-level practices in a clear, NIST Cybersecurity Framework-aligned approach. SP 800-161 is dense, but it gives both procurement, security and engineering an aligned vocabulary-which is often the first battle to get won.

NIST SP 800-218 Secure Software Development Framework establishes standard practices that software producers must follow [9]. Executive Order 14028 Secure Software Development (May 2021) made adherence to SSDF conformance and use of software bills of materials requirements that U. S. Federal government procurement must use when acquiring software [10].

The result is indirect but real. Vendors that sell to both the U. S. Government and the commercial sector typically do not segregate product development and apply the same practices to both customers.

The international standard IEC 62443-2-4 Industrial Automation and Control Systems: Security Controls for System Service Providers, Industrial Automation and Control Systems, defines a standard that integrators and original equipment manufacturers must comply with, allowing pipeline operators to write it into contracts as security requirements [11]. These standard documents-62443-4-1 Product Requirements, 62443-4-2 Product Requirements and 62443-3-3 System Requirements-should all be reviewed to varying degrees by operators and integrators alike.

The sector-specific guidance documents are far more diffuse and less harmonized than in other sectors. American Petroleum Institute Standard 1164 Pipeline SCADA Security was revised in 2021 and is now considered current with its guidance on network segmentation and remote access [12]. TSA pipeline security directives issued in 2021 and 2022 require specific security incident reporting and architectural reviews and have direct impacts on operators' vendor management [13]. No individual guidance documents stand in isolation. Operators use NIST SP 800-161 as the primary guideline and adapt from other sector-specific documents as it helps refine a control, as an individual directive cannot fully address all risk controls.

5. A Practical Vendor Risk Program

Figure 3 shows the lifecycle that programs converge on once they have run for a few years. The stages are not novel. What is hard is running them at scale, against hundreds of vendors, with engineering and procurement participating rather than handing the work back to security.



Figure 3. A Vendor Risk Lifecycle. Continuous Monitoring Feeds Back into Reassessment and May Trigger Contract Amendments or Access Changes

5.1. Identify and Inventory

The first part of it is not sexy. It is what most programs cannot get right. You have to know or have some measure of confidence about which vendors or service providers have Logical or physical access to your environment. Logical access means administrator credentials on domain controllers and even includes service accounts for historians. Physical access means a tech service plugging into a laptop on an engineering workstation during turnaround? Look at your procurement records, identity databases, access logs for jump servers, badge readers and cross-reference as best as you can. The list is never fully done, it is what gets better and better as you go.

5.2. Tier and Assess Risk

Vendors differ greatly, while many vendors (say, those selling pipe coatings) do not need such extensive testing, some vendors, for example, vendors selling access to control rooms remotely, should. In these cases, the depth of due diligence ought to correlate to the potential impact of a cyberattack involving the vendor. A perfectly acceptable tiered method would consist of a three-tier scheme, taking into consideration: the potential logical access of the vendor (does the vendor gain access to the OT? Does the vendor have elevated credentials for OT?), the criticality of the vendor's operations on the systems involved (e. g. , safety vs. Production vs. Business process systems) and the capability of the company and operators to manage the attack if it originates from this vendor.

5.3. Contract Requirements

Contracts offer to control the behavior of OT vendors, mature programs often include breach notification language demanding a certain number of days' warning to OT-side stakeholders, software bill of materials delivery on request, secure software development certifications or attestations of adherence, restricted access requirements, the right to audit at the OT owner's discretion, indemnification, continuing after the expiration or termination of the contract. Today none of these points is outside the realm of reasonable demands on software supply chain vendors, but they often fail to be in OT security or supply

chain contracts. One old contract is still in use, it does not contain some of the modern provisions, many are in place but poorly written.

5.4. Onboard and Integrate

All vendor access should be handled by your current identity and privileged-access infrastructure as your own users. Dump your shared accounts, use distinct identities. Always tunnel remote vendor access to OT systems through the jump hosts. Remote vendors need posture assessment of their machines before being allowed to access the OT environment, without being given the run of your network. Contract terms are actualized in your vendor onboarding process. That handover between procurement and IT/OT is the point where it gets really hard or gets really lax.

5.5. Monitor and Reassess

Monitoring has two fronts. First, look at the vendor security posture using threats, breaches and service ratings. Second, look at the vendor's activities within your environment via session logs, jump server records and SIEM analysis. Either finding should prompt re-evaluation and as needed, changes to the contract or access. An annual re-assessment is reasonable, but event-driven reassessment is what will expose risks before they harm you.

6. Open Problems

I would not claim we are near the end, nor should anyone else claim to be, especially to program stakeholders (whom programs will always need).

Even in industrial environments, it is often hard for users of software packages to tell whether they depend on open source and what components are actually included in them. While vendors are getting better, the Software Bill of Materials produced (which lists these components) has poor standards in terms of content, format and whether machine tooling can use it. It is hard for an operator who would like to automate ingestion and continuous correlation against vulnerability data from many sources to make it work.

The industrial software vendors have narrowed their market into many niche areas. Even a single OEM whose systems are compromised could bring down significant amounts of the world's industrial infrastructure in many places and industries at once. As this is an industry-wide risk, no one operator can solve it. Mitigations include diversifying vendor supply to reduce that dependence as much as possible, performing detailed inspections (not merely reliance on marketing claims) of the vendors that a company does rely on and working closely with sector-specific information sharing bodies (ISACs and the like) to gather intelligence.

Operators, however, must be honest about the limited scope of due diligence, as I have argued at various points previously. Filling in the correct boxes in a questionnaire does not constitute security. Any company that over-prioritizes the paper trail of security will likely de-prioritize spending on the controls (identity management, network segmentation and incident monitoring systems) that will be needed to stop breaches of vendor systems when they happen.

7. Conclusion

Supply chain risk is not a category outside of the security team. The supply chain is another area in which an external attack vector exists, and the supply chain must be protected using the same architecture as every other area. It became glaringly obvious to organizations worldwide from 2020 to 2022 that security in supply chain risk had been ignored. Frameworks were produced in parallel: so at least now people can speak intelligently about supply chain risk. Supply chain programs have a bunch of boring things that must be done: take inventory, tier suppliers, put contracts in place, manage supply chain access, watch post-award procurement processes. Those vendors who see the program as a yearlong (or more) journey will not be the ones whose companies get cited in the postmortems of the future.

References

[1] U.S. Cybersecurity and Infrastructure Security Agency, “Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations,” Alert AA20-352A, December 2020.
[2] U.S. Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, “Kaseya VSA Supply-Chain Ransomware Attack,” Alert AA21-209A, July 2021.
[3] U.S. Cybersecurity and Infrastructure Security Agency, “Apache Log4j Vulnerability Guidance,” Alert AA21-356A, December 2021.
[4] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,” NIST Special Publication 800-161 Revision 1, May 2022.
[5] European Union Agency for Cybersecurity (ENISA), “Threat Landscape for Supply Chain Attacks,” July 2021.
[6] U.S. Cybersecurity and Infrastructure Security Agency, “Defending Against Software Supply Chain Attacks,” guidance document, April 2021.

[7] U.S. Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, “DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks,” Joint Advisory AA21-131A, May 2021.
[8] U.S. Cybersecurity and Infrastructure Security Agency, Department of Energy, Federal Bureau of Investigation, and National Security Agency, “APT Cyber Tools Targeting ICS/SCADA Devices,” Joint Advisory AA22-103A, April 13, 2022.
[9] M. Souppaya, K. Scarfone, and D. Dodson, “Secure Software Development Framework (SSDF) Version 1.1,” NIST Special Publication 800-218, February 2022.
[10] The White House, “Executive Order 14028: Improving the Nation’s Cybersecurity,” May 12, 2021.
[11] International Electrotechnical Commission, “IEC 62443-2-4: Security Program Requirements for IACS Service Providers,” 2015 with amendments.
[12] American Petroleum Institute, “API Standard 1164: Pipeline Control Systems Cybersecurity,” third edition, 2021.
[13] U.S. Department of Homeland Security, Transportation Security Administration, “Security Directive Pipeline-2021-01 and Pipeline-2021-02 (revised),” 2021–2022.
[14] Verizon, “2022 Data Breach Investigations Report,” May 2022.
[15] National Telecommunications and Information Administration, “The Minimum Elements for a Software Bill of Materials (SBOM),” July 2021.
[16] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1, April 2018.