IDI
Billing Solutions

Unraveling The Tangled Web:
The Importance Of Supply Chain Risk Management For Telecom Service Providers

In today's fast-paced world, telecom service providers play a vital role in ensuring seamless connectivity and communication. However, just like any other industry, they are not immune to risks and uncertainties. With the increasing dependence on software solutions and the growing complexity of supply chains, it becomes essential to implement effective risk management strategies.

Supply chain risk management for telecom service providers is crucial in maintaining a robust and reliable network infrastructure that supports the needs of customers, businesses, and society as a whole. By understanding the types of vendors that pose risks, implementing effective risk management strategies, and adopting best practices, these service providers can navigate the complexities of their supply chains with confidence.

The Rise of Supply Chain Attacks

More than three fifths of US businesses have been directly affected by a software supply chain threat over the past year.* And while supply chain attacks didn't begin in the last three years, the SolarWinds hack in 2020 and the Log4j attack in 2021 brought a lot of attention to the threats and impact of software supply chain issues.

The SolarWinds hackers used a method known as a supply chain attack, involving the targeting of a third-party entity with access to an organization's systems instead of directly breaching the network, and embedded malicious code into the SolarWinds Orion platform. When SolarWinds sent out fresh software as an update or patch, the hacked code created a backdoor to customer's information technology systems, gaining them access to networks, systems, and data of thousands of SolarWinds customers — including government agencies.

Log4j is an open-source logging framework that is used to log messages within software and is able to communicate with other services on a system. In 2021, malicious code was injected into the logs by an attacker, affecting millions of applications and devices across the globe. While the use of open-source software (OSS) platforms and components has streamlined software development for organizations, it opens the door to detrimental vulnerabilities like the Log4j attack.

Different Vendors Pose Different Risks

Telcos rely on various vendors to ensure the availability and functionality of their network infrastructure. It is essential to identify and assess the risks associated with these vendors to avoid potential disruptions to services. Different types of vendors pose different types of risks.

Initial/primary vendors: These vendors supply critical components or services directly related to the core operations of service providers. Any disruption or failure in this tier can have severe consequences.

Secondary vendors: These vendors often provide non-core components or services, but their role is still significant. Disruptions at this level can impact service quality, maintenance, or introduce security vulnerabilities.

Tertiary or managed service providers: These vendors are typically third-party entities engaged by telecom service providers to manage specific functions or processes. While outsourcing certain aspects can improve efficiency, it introduces new risks that need careful consideration.

Understanding the potential impact of each vendor within the supply chain is crucial for devising effective risk management strategies. But it's not just about who your vendors are — as the name suggests, a thorough supply chain risk management strategy looks at the entire supply chain. Getting a better understanding of your vendors and the software and suppliers they rely on is key to developing a more holistic risk management strategy.

According to Capterra, 94% of companies use at least one fully open-source platform, and 57% of companies use multiple. With the recent uptick in supply chain attacks, like the aforementioned Log4j hack, concerns about OSS are rising, and companies and government agencies are looking for ways to mitigate the risk. One technique is to provide a Software Bill of Material (SBOM). Similar to a bill of materials in traditional manufacturing, an SBOM provides a comprehensive listing of the software components used in an application or system and can be provided to customers so they can understand their supply chain, and what vulnerabilities might be embedded inside the software they use.

Implementing SBOMs in supply chain risk management strategies enhances the industry's ability to evaluate the security posture of software vendors. By having a clear understanding of the software components and their dependencies, telecom companies can identify vulnerabilities or potential threats and take appropriate actions to mitigate them. SBOMs are gaining significant attention in the realms of supply chain risk management, with 49% of businesses requesting an SBOM from their vendors as part of their supply chain defense strategy.

The Significance of Supply Chain Risk Management for Telcos

Supply chain risk management is more than merely a mitigative measure for service providers; it is a vital component in ensuring uninterrupted service delivery and safeguarding against potential disruptions. By embracing effective risk management practices, service providers can:

Minimize Downtime

Proactive risk management helps identify vulnerabilities and implement contingency plans to minimize the impact of disruptions. This enables service providers to deliver uninterrupted services and meet customer expectations.

Enhance Customer Trust

By implementing robust risk mitigation measures, service providers can demonstrate a commitment to reliability and customer satisfaction. This fosters trust among customers and strengthens their loyalty to the brand.

Protect Revenue Streams

Network outages or disruptions can lead to financial losses for both service providers and their customers. By effectively managing the supply chain risks, telecom service providers can protect their revenue and maintain healthy financial standing.

Ensure Compliance

The United States government aims to strengthen cybersecurity defenses across various sectors, with a new focus on software companies, according to Executive Order 14028. Organizations that sell to federal agencies or are involved in the supply chain to federal agencies must comply with the National Institute of Standards and Technology (NIST) guidelines. This new inclusion highlights the critical role played by software vendors in the telecom industry's supply chain and the need to manage associated risks effectively.

As part of the initiative to ensure every American has access to high-speed internet, the NTIA Broadband, Equity, Access, and Deployment (BEAD) Notice of Funding Opportunity outlines specific cybersecurity and cyber supply chain risk management rules that states must require of their subgrantees. Telcos looking to receive BEAD grant funds must meet these specific supply chain risk management requirements.

Best Practices for Establishing a Supply Chain Risk Management Plan

In the digital world, the incorporation of digitalization, workflow automation, and the fusion of these workflows with the physical world through the Internet of Things (IoT) is imperative for advancing supply chain optimization in the next generation. However, relying solely on a reactive approach to managing supply chain risks falls short. A proactive risk management strategy for both your supply chain and your relationships with suppliers is vital for satisfying stakeholders, safeguarding and fortifying business partnerships, and fortifying your resilience against supply chain disruptions that could potentially incapacitate or even devastate your business.

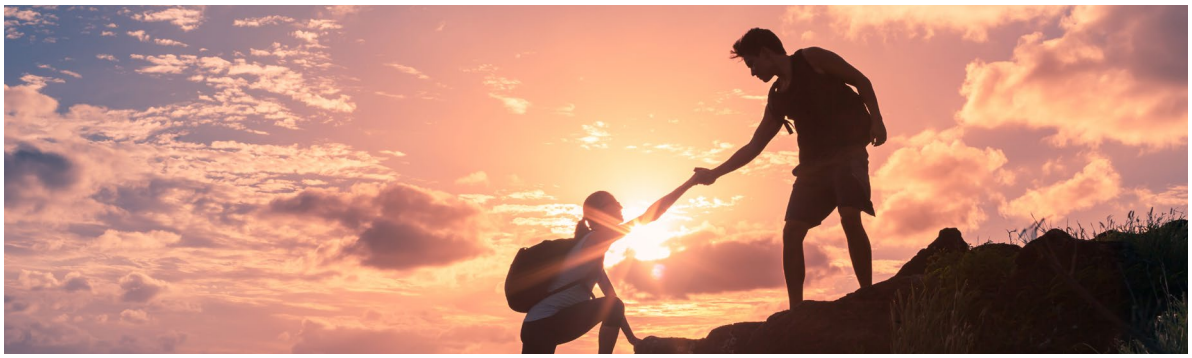
Devising an effective supply chain risk management plan requires a comprehensive understanding of potential vulnerabilities and proactive measures to mitigate these risks. To establish a robust plan, telcos should consider implementing the following best practices outlined by NIST:

- Integrate Cyber Supply Chain Risk Management (C-SCRM) Across the Organization
- Establish a Formal C-SCRM Program
- Know and Manage Critical Components and Suppliers
- Understand the Organization's Supply Chain
- Closely Collaborate with Key Suppliers
- Include Key Suppliers in Resilience and Improvement Activities
- Assess and Monitor Throughout the Supplier Relationship
- Plan for the Full Life Cycle

Each Key Practice has additional recommendations that describes how people, processes, and technologies can be utilized to assist and support the implementation of an effective C-SCRM program, including:

- Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, physical security, and other relevant functions.
- Integrate cybersecurity considerations into the system and product life cycle.
- Determine supplier criticality by using industry standards and best practices.
- Mentor and coach suppliers to improve their cybersecurity practices.
- Include key suppliers in contingency planning (CP), incident response (IR), and disaster recovery (DR) planning and testing.
- Use third-party assessments, site visits, and formal certification to assess critical suppliers.

These recommendations outlined by NIST can be used as a guideline to help organizations of any size implement a robust, holistic supply chain management program.



Security Needs Are Evolving, Trust In IDI To Facilitate Risk Management

Supply chain risk management plays a vital role in ensuring the security and stability of the telecom industry. As technology continues to evolve, it is crucial for telecom service providers to stay ahead of potential risks and ensure the reliability and resilience of their supply chains – and that starts with looking at their primary vendors.

As a leading Billing & OSS solution for telecom service providers, IDI Billing Solutions understands how vital it is for vendors of telcos to prioritize cybersecurity measures and maintain a supply chain risk management program of their own. IDI's Third-Party Provider Management Policy sets standards and guidelines for selecting vendors, performing vendor risk assessments, and ongoing monitoring of contractual associations with our vendors. Our supply chain risk management program establishes controls for identifying, measuring, approving, monitoring, and managing risks of third-party vendor agreements.

In addition to annual information security risk assessments performed by IDI's Security and Risk Management team, additional risk assessments are used to identify aspects of the environment that need to be checked on a regular basis, along with developing a plan for how frequently they need to be checked, who is responsible, and how the risk will be removed or minimized.

By adopting a proactive and strategic approach to supply chain risk management, IDI is able to inspire customer confidence, protect their revenue streams, and maintain their position as industry leaders.

Build A Better Security Experience With IDI.

Since our inception nearly 30 years ago, IDI has made security and trust a top priority — we have significantly invested in people, processes, and technology to ensure our customers' data is protected, and that our solutions are trusted and reliable. IDI maintains a robust security program based on the NIST CyberSecurity Framework and we continue to maintain strict adherence to the highest certifications to compliance framework controls, including SOC1/SSAE 18, SOC2 (Security, Availability, Processing Integrity, Confidentiality, and Privacy), PCI DSS, and HIPAA.

If you're interested in learning more about IDI's security and supply chain risk management programs — or if you just have some questions or would like to share your thoughts — we'd love to hear from you.

To learn more, call **888.924.4110**, or contact us **here.**