Supply Chain Risk

WHITE PAPER

May 2023

VERSION: 1.0

TABLE OF CONTENTS

Introduction

In today's interconnected world, supply chain security has become an essential element of cybersecurity.

As businesses increasingly rely on third-party vendors and suppliers, the potential for a breach or attack through the supply chain has become a significant concern.

Organisations must understand the security implications of their supply chain and implement suitable controls to mitigate risks.

There are several reasons why supply chain security needs your attention today:

Increased Interconnectedness: Modern supply chains are highly interconnected, involving multiple vendors, suppliers and partners. Each entity in the supply chain represents a potential entry point for cyber threats. Weaknesses or compromises at any point can be exploited to infiltrate the entire supply chain, making it crucial to secure every link in the chain to protect the overall ecosystem.

Third-Party Risks: Organisations often rely on third-party vendors and suppliers for components, software or services. But this reliance introduces additional security risks. A compromise or breach within a third-party supplier can have cascading effects on the organisation and its customers. Ensuring robust security measures throughout the supply chain is essential to mitigate risks associated with third-party vulnerabilities.

Attack Surface Expansion: Cybercriminals are increasingly targeting the supply chain as an attractive attack vector. By compromising a trusted supplier or injecting malware into the supply chain, adversaries can infiltrate target organisations without direct attacks. This expands the attack surface, making it imperative for organisations to implement stringent security measures across the supply chain to minimize the risk of unauthorized access or data breaches.

Counterfeit and Tampered Products: Supply chain security also mitigates risks posed by counterfeit or tampered products. Unauthorised modifications or substitutions within the supply chain can lead to compromised products or malicious software embedded in hardware or software components. Ensuring supply chain integrity helps safeguard against distribution of counterfeit or tampered products that could result in financial loss, reputational damage or compromise of sensitive information.

Regulatory and Compliance Requirements: Many industries and jurisdictions have introduced regulations and compliance standards that emphasise supply chain security. Meeting these requirements is essential to avoid legal penalties and maintain trust with customers, partners and regulatory bodies. Organisations need to demonstrate robust supply chain security practices to comply with industry-specific regulations, such as those governing data privacy, financial services and healthcare.

This paper aims to provide guidance on how customers can understand supply chain risks and implement suitable controls.

Background

A supply chain is a network of organisations, individuals, resources, and activities involved in the creation and delivery of a product or service to the end customer (both directly and indirectly).

The supply chain can be complex and involve multiple tiers of suppliers, making it challenging to assess and manage the risks.

Supply chains face various threats, such as cyber-attacks, physical attacks, theft, fraud, counterfeiting, and natural disasters.

These threats can have significant consequences, including loss of data, financial loss, reputation damage, and disruption of operations.

The cyber security of your organisation, your data and the ability of your organisation to deliver are all likely to have a dependency on the cyber security of your supply chain.

Specific examples where vulnerabilities in the cyber security of your supply chain could impact your organisation:

- An organisation processes your staff and customer data is compromised resulting in the disclosure of your data, reputational damage and regulatory fines.
- An organisation that supports your IT systems is compromised and provides a backdoor into your systems.
- An organisation that provides a critical (hardware) component as part of your manufacturing process is compromised and subject to ransomware attacks which cripple their supply capability.
- An organisation that provides you with software is compromised - and their software includes backdoor accounts that can be remotely accessed.

A recent high-profile example of a supply chain attack is the 2020 SolarWinds supply chain attack, which affected multiple organisations, including government agencies and major technology companies.

Supply Chain Risks

The first stage in understanding your supply chain risks is to assess your organisation's critical information assets, systems, and services and where your supply chain fits into this.

In the same way organisations carry out a cybersecurity risk assessment internally, they should also extend this to cover external supply chains.

To avoid duplication and promote consistency and reporting transparency, it makes sense to use a common risk assessment methodology internally and across your supply chain.

When assessing risks across supply chains, it may make sense to group risk assessments to cover multiple suppliers providing similar services.

However, if adopting thisapproach, ensure you take into consideration differences in the risk profile due to factors such as the geographical location of a supplier.

When assessing the risks of your supply chain you should consider:

- What data and trade secrets your supplier has access to and processes on your behalf
- What hardware and software systems your supply chain provides
- What access your supply chain has to your systems
- How dependent you are on the hardware,software and services supplied by your supply chain, and how a loss of these services would impact your business

A supply chain risk assessment should include the following steps:

1. Identify the critical components of the supply chain that are essential to the organisation's operations and determine their importance. [NOTE:How – on a scale of 1-10, for example?]
2. Identify potential risks and vulnerabilities associated with each component, such as cyber attacks, theft, fraud, natural disasters or political instability.
3. Evaluate the likelihood and impact of each risk on the organisation, including financial loss, reputational damage, operational disruption and regulatory non-compliance.
4. Prioritise risks based on their potential impact and likelihood – then develop a risk management plan.

Managing Supply Chain Risks

Once you have understood the risks to your supply chain, you can then look at managing those risks.

Management of supply chain risk should be aligned with your organisational risk appetite, in a similar way to how you manage risks to your internal organisation.

A risk-based approach should be taken: apply the most effort and controls on those parts of the supply chain that pose the highest level of risk to your organisation.

Controls should be relevant and proportionate.

Contracts

Security contracts are an essential means for ensuring security requirements are clear and concise. The contract should cover the set-up operation and handover of the service at the service's end from suppliers within your supply chain.

Compliance Frameworks

Compliance frameworks provide a common, predetermined set of requirements and independent assessment for the implementation of controls. Theycan be applied to supply chains as a baseline standard. Specific examples of compliance frameworks include:

- CE and CE Plus

- ISO/IEC 27001
- PCI DSS

A Sector-Based Approach

A sector-based approach involves developing sector-specific security guidelines and best practices.

A sector-based approach allows buyers and regulators to influence suppliers and vendors to address industry-specific risks.

A specific example of a sector-based approach is TISAX (Trusted Information Security Assessment Exchange). This is a framework for information security assessments in the automotive industry. It was developed by the German Automotive Industry Association (VDA) and is based on the international standard ISO/IEC 27001 for information security management systems.

TISAX provides a standardised and secure method for exchanging information about information security assessments between automotive companies and their suppliers. It is designed to ensure all companies in the supply chain meet the same high level of security standards, and can provide evidence of this through a standardised assessment process.

Targeted Controls

There are several targeted controls that can achieve targeted assurance and treat supply chain risks. They can be included as part of contractual requirements or compliance requirements. Specific examples include:

Penetration Test

Evidence of 'pen testing' from a reputable accredited testing organisation such as a CREST-accredited pen testing company provides a quick and effective way to provide assurance that the supply chain's public and internal systems are free from known security vulnerabilities and configuration errors.

When looking at an organisation's penetration testing regime, the scope of testing and frequency should also be reviewed.

Threat Hunting

Threat hunting involves actively searching for threats and indicators of compromise within an organisation's systems and networks.

It helps detect and respond to threats before they cause significant damage.

Especially if you are an organisation working in a high-threat context such as defence, then threat hunting can provide a level of assurance that any organisation within your supply chain has not been compromised prior to authorising any direct

connectivity with your networks, or before providing them with sensitive IPR and/or trade secrets.

Communities of Interest and Threat Intelligence Sharing

Joining communities of interest and sharing threat intelligence can help organisations stay up to date on the latest threats and trends in the specific industry, and help address emerging threats that may impact your supply chain.

Vetting

By requiring staff vetting among companies on your supply chain, you can reduce the risk of security breaches that could result from an insider threat.

This can help protect sensitive data, intellectual property and other valuable assets.

Examples of where this should be considered is when your suppliers have direct access to your systems or large volumes of sensitive, sensitive personal data, and trade secrets -- or are involved in financial transactions.

Insurance

Cyber insurance can provide financial protection in the event of a cyber-attack or data breach and help ensure the supply chain organisation is resilient in the event of an attack.

Product Assurance

If a supply chain organisation is providing a security=critical component, then product assurance can mitigate risks to that component in terms of ensuring it operates as expected, and is free from known vulnerabilities and embedded malicious code or backdoors.

Examples of formal product assurance schemes include Common Criteria.

Code Reviews and SDLC Frameworks

Code reviews and Software Development Life Cycle (SDLC) Framework Assessments involve reviewing the source code of software and the development lifecycles to identify potential vulnerabilities and weaknesses. Requesting that code reviews and SDLC Framework Assessments are conducted by organisations within your supply chain provides a means of assuring security-critical software is securely designed and developed, and free from known vulnerabilities, malicious code and backdoors.

Cyber Incident Response Capabilities

Ensuring your supply chain has effective cyber incident response capabilities in

place helps ensure that incidents impacting your organisation and supply chain are more likely to be detected and responded to in an effective, timely manner.

Escrow

Escrow involves depositing source code, documentation, and other critical materials with a third-party provider. It can help ensure you can access these mission-critical materials if a supplier goes out of business or fails to deliver.

Monitoring and Continuous Improvement

An effective supply chain security regime should include on-going mechanisms for:

- Managing compliance
- Measuring the effectiveness of controls, and
- Initiating corrective and preventative action where required.

This should occur as part of periodic reviews (such as annual checks) as well as a result of specific, identified triggers such as an incident, contract renewal, a significant change in services provided or a change in threat level.

Further Support

If you need assistance in designing, implementing, or complying with supply chain security frameworks and supporting controls then the specialists at AMR CyberSecurity can support you. Please contact enquiries@amrcybersecurity to speak to one of our consultants.