ADVANCED CYBER DEFENCE SYSTEMS

ESSENTIAL GUIDES **NO.2**

An introduction to: SUPPLY CHAIN SECURITY

Don't Be The Weak Link: Read our essential non-techie guide to supply chain cyber security

Author: Elliott Wilkes

Table of Contents

Introduction

Don't Be The Weak Link:
A Non-Techie Guide To Supply Chain Cyber Security

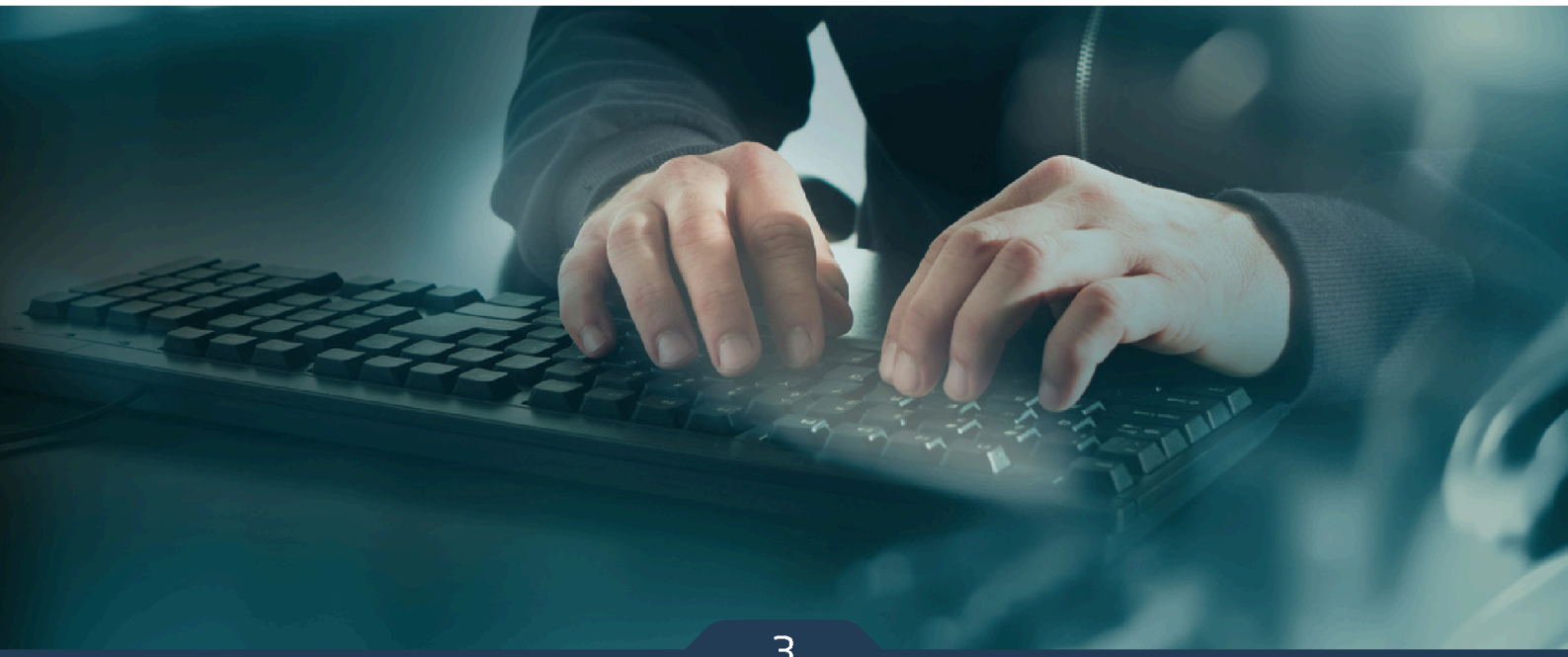
Every supply chain has weak spots and vulnerabilities. And when it comes to supply chain cyber attacks, threats are becoming more prevalent and more complex.

Any business can now be the subject of ransomware attacks or data breaches, which means investing in proper security management systems is essential not only for your own business but also for all your stakeholders, suppliers and customers.

Your strength as an organisation is contingent upon the resilience of your suppliers. Organisations must vigilantly monitor all suppliers and ensure they commit to a strong cybersecurity posture.

Attackers often exploit vulnerabilities in weak suppliers to breach their intended targets. Fostering a culture that incorporates cyber security into every business area, across the entire supply chain is paramount.

Just as importantly, it is crucial for your organisation to avoid becoming the weakest link. That can have devastating repercussions on the relationships with your suppliers and customers.



What Is Supply Chain Cyber Security?

A supply chain functions as an interconnected series of links, where each link represents a different stage of the process.

A supply chain encompasses the entire journey of a product or service, from its creation to its delivery, involving different stages, locations, and activities along the way.

To be secure, an organisation needs every link in their supply chain to maintain a strong cyber security posture. If a particular supplier lacks sufficient cyber security measures, this could leave them and the entire supply chain open to attack. The stronger the supply chain cyber security, the less likely you are to fall victim to malicious activity.

Why Supply Chain Attacks Are On The Rise

With the expanding digital landscape, there are more entry points for attackers to target and exploit.

Digital transformation efforts have been booming and that means migration of systems to new hosting configurations along with the rapid development of customer-facing sites and technologies. All of these represent potential areas of misconfiguration and vulnerability that attackers look to exploit.

Additionally, supply chains have grown increasingly interconnected due to advancements in technology. Attackers now recognise the lack of budgetary resources available for smaller businesses to invest in cyber security compared to larger organisations, making them appealing targets to cybercriminals.

They strategically target these weaker organisations with the aim of bypassing their defences and reaching larger targets.

One of the most significant threats to an organisation is failing to conduct thorough audits of their supply chain, therefore giving cybercriminals nice and easy access to their organisation through their weaker suppliers.

According to Cyber Security Breaches Survey 2022 (GOV.UK): "Just over 1 in 10 (13%) of businesses review the risks posed by their immediate suppliers, and the proportion for the wider supply chain is half that figure (7%). Charities are even lower (9% and 5% respectively)."

As the tactics of cybercriminals grow increasingly sophisticated, they have recognised the potential of targeting the supply chain. By attacking a single link within the chain, these criminals gain access to many other organisations in a single hit, magnifying the impact of their actions.

The Most Popular Types of Supply Chain Attacks

There are various types of supply chain attacks which are frequently used by cybercriminals. A few examples are:

Malware

Malware is malicious software designed to modify code and systems without a user's control. It plays a critical role as it is a key tool used in supply chain attacks. Attackers deploy diverse tactics to target organisations with malware; this includes exploiting vulnerabilities, gaining unauthorised access, or using social engineering techniques, such as phishing, to infiltrate systems deceitfully.

Malware can be injected into legitimate software or firmware in the form of trojans, backdoors, keyloggers, malicious payloads etc... and look undetectable by the end user. Attackers that use malware in supply chain attacks prey on the trust between suppliers to infiltrate and manipulate the supply chain.

Firmware

Firmware is low-level software embedded in hardware devices, like printers, routers, CCTV systems and more. Through a breach of the manufacturer's system or exploiting vulnerabilities in the supply chain (like software packages used to comprise the ultimate firmware package), firmware can be targeted by attackers to inject malicious code. This can then provide the attackers unauthorised access to the supply chain.

The firmware can be installed onto the hardware devices and widely distributed. The danger of this can be if other organisations within a supply chain have these compromised devices, the attackers can gain unauthorised access to their target organisation's network.

Compromised Software

Compromised software is a common vector used in supply chain attacks. This can occur by infiltrating the software supply chain, e.g. compromising the software during the development, distribution or update process. Malicious code can also be injected into legitimate software that is used by the supply chain.

Once this software has been compromised, it can be distributed as normal, as if it was a legitimate update which users will unknowingly download and install. Once inside these systems, attackers can attack the supply chain using various techniques.

Weak Spots In Your Supply Chain Security

An Example Of A Convincing Supply Chain Attack

A recent and ongoing supply chain attack, widely recognised as the 'MOVEit' breach, has left a trail of victims, including notable giants like Boots and British Airways, among numerous other prominent corporations.

At the end of May 2023, the data transfer company, MOVEit, identified a potential threat, a zero-day vulnerability relating to SQL injection. This vulnerability has affected more than 200 organisations in their supply chain, a perfect example of how one attack can impact multiple entities.

This breach stands as one of the most significant supply chain attacks to date, and each link that has been impacted in the supply chain has been faced with severe consequences, including damaged reputations, loss of trust, and substantial financial ramifications.

The Real-World Costs of Poor Cyber Security

Poor cybersecurity can lead to significant real-world costs, from internal troubles to external issues with suppliers.

There are also different consequences depending on the type of business. The top real-world costs include:

- Financial loss
- Reputational Damage
- Supplier relationships impacted
- Disruption of operations
- Legal costs

Reputational damage to a large organisation can profoundly impact customer loyalty which can result in a number of different problems. Once customer trust has been lost, it may prompt them to seek alternative services, resulting in long-term financial implications.

It can also cause strained relationships with suppliers, and with diminished trust, it may result in them opting not to collaborate with you in the future. Amongst these issues, the disruption of operations can halt business activities, causing a cascading effect throughout the supply chain. Not to mention legal expenses, as breaching data protection laws often involves legal repercussions, with organisations facing fines and potential legal action against them.

The initial financial loss is an evident concern, but the aforementioned, broader impacts can exert even more significant financial ramifications over time. In some cases with small/medium-sized organisations, a cyber attack can disrupt a business to such an extent that it cannot recover at all.

The Benefits Of Bolstering Your Supply Chain Cyber Security

If your organisation does not have a strong enough cybersecurity posture, the time to act is now. Don't be the weak link.

It is also equally as essential to not allow other suppliers within your supply chain to be vulnerable access points for attackers due to inadequate cybersecurity measures. Advancing your supply chain security offers three key benefits:

- Risk management
- Reputational trust (for customers and suppliers)
- Business continuity

If your organisation falls victim to a cyber attack, there is a high chance that customers and suppliers will question your ability to safeguard their data and often seek alternatives. In some cases, business operations are halted, and this delay can have catastrophic impacts; by implementing sufficient cybersecurity measures, business continuity can be protected for you and your supply chain.

Cyber security is not just a technical issue; it is a critical aspect of risk management. By effectively managing cyber security risks, the overall risk exposure of your company declines.

Supply Chain Security Guiding Principles: A Supply Chain Cyber Security Framework

There are a few steps that an organisation can take to enhance their supply chain cyber security, and adhering to these guiding principles can set you up on the right path.

1 Identifying and understanding the risks

If supply chain risks have not been identified previously, it may prove time-consuming, but it is incredibly worthwhile. The initial step involves understanding what needs to be protected and why.

Gaining clarity on identifying all suppliers is crucial to gauge the level of risk and value of information or assets they hold. It is equally important not to overlook sub-contractors associated with each supplier too.

2 Establish control of your supply chain

Start by effectively communicating your security needs to suppliers; establishing control of your supply chain involves thoroughly assessing each supplier's adherence to security expectations.

Extra caution should be taken for those suppliers that have access to critical assets, and different protection requirements should be dealt with on a case-by-case basis. Remember to meet your own security requirements as a supplier and consumer.

3 Continuous improvement and maintenance

Creating awareness about the criticality of each link having a strong cyber security posture will foster a culture of best practices. Once each supplier has been acknowledged and assessed, it is important that they continue to enhance their level of protection and keep up to date with the latest threats.

Reinforce to your suppliers the significance of supply chain security in solidifying the trust and collaboration between each other.

Your 5-Step Cyber Check: How To Audit Your Current Set Up

Conducting an audit on your current supply chain is integral. ACDS' **Chief Technology Officer, Elliott Wilkes**, gives his advice on how to audit your current set-up

1 Identifying and understanding the risks

First, you need to build a list of your assets and vendors, being sure to capture how each device or system accesses, manages, processes, and stores your organisation's data.

2 For each asset and vendor, review the data housed in each and the associated risks

Next, make sure to record the type of data involved in each (i.e. Personal Identifiable Information (PII), core business intellectual property, financial details, etc.) and the associated level of risk if the system were to be compromised.

You can start with a matrix evaluating risk as the impact of a breach (High: major business disruption, Medium: business disruption but recovery, Low: little impact).

For systems that process your most sensitive and critical data with the highest impact in the event of a breach, ensure you dedicate energy and resources to defend them commensurate with the risk a breach poses to your organisation.

3 Request All Current and Future Suppliers Complete Self-Assessment

In this case, a self-assessment can often be in the form of a questionnaire that vendors are required to complete, which lists best practices in cyber security and asks if they adhere to them. If not, the vendor should be given an opportunity to explain.

The key is having a written record of security processes to validate that they are responsible for handling data and investing appropriately in their cyber security measures.

For more mature organisations, adherence to these can be included as terms of their contract.

A critical part of understanding and minimising the cyber risks to your supply chain is ensuring that you manage the procurement process.

Going forward, all new contracts should have a cyber security review (like a self-assessment) as part of due diligence before signing. This ensures that you don't introduce unexpected or uncaptured risks by onboarding new suppliers that don't adhere to industry best practices in cyber security.

4 Establish a regular cadence for audits of the data stored and processed in your assets and by your vendors

You can have higher confidence in your security measures when they are tested. Using a firm to conduct penetration testing of your systems is a good way of highlighting configuration issues and finding problems or weaknesses in your systems.

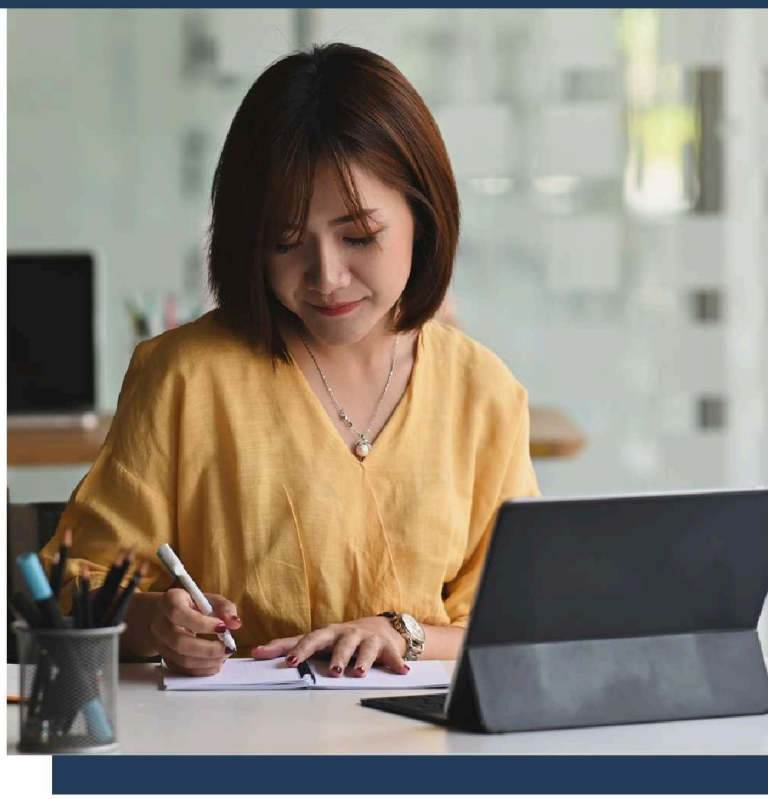
Depending on the size of the organisation, you can ask for an independent audit of your supplier's security practices, including a penetration test.

Bigger organisations do these regularly and will be able to provide you with the reports on request. Smaller companies might need you to cover the cost of this, but it is a worthy investment if they have significant risks posed to your data.

Regular audits also should entail the above assessment of data, ensuring that you always have an accurate picture of what data is stored where and how it is protected.

5

Write an incident response plan covering your vendors and practice it



The best incident response plans are ones that are practised so that when an actual incident occurs, the team understands the flow and has experience in assembling the relevant people. By enabling them to make decisions, they can take appropriate actions like limiting the impact of a breach, suspending suspicious accounts, and restoring systems from backups.

One of the most common things organisations forget is planning for cyber security incidents— attacks are more and more frequent these days, so having a plan in place is a necessary component of a resilient organisation's cyber security posture.

A good plan will list key actors and administrators for critical systems with contact details, a single point of contact (decided at the time of the incident) to manage the incident investigation and response, and decision paths laid out clearly for different severity scenarios.

Useful Links:

The UK Government's **National Cyber Security Centre** has a good playbook for this work:
https://www.ncsc.gov.uk/collection/10-steps/incident-management

Also, the US Government's **Cybersecurity and Infrastructure Security Agency** has this report on securing your supply chain:
https://www.cisa.gov/sites/default/files/202304/building_more_resilient_ict_supply_chains_factsheet_508.pdf

UK NCSC Supply Chain Security:
https://www.ncsc.gov.uk/collection/10-steps/supply-chain-security

Protecting Your Business With Cyber Insurance

In this time of constantly evolving cyber threats, cyber insurance has become a crucial necessity.

However, this should not be included as a layer of protection against an attack. Instead, it compliments multiple layers of cybersecurity measures, working in tandem to enhance protection and response. *There are many benefits to having cyber insurance, which include:*

Financial Protection

Cyber attacks can incur substantial financial impacts. Without insurance, many organisations would not be able to recover a significant portion of the costs associated with the attack. These costs extend beyond ransomware payments or business disruption and may include expenses for investigation, legal fees, regulatory fines, and potential lawsuits.

Legal Support

There are often complex legal considerations that need to be accounted for, which usually result in hefty expenses. Organisations may face legal and regulatory consequences, and having insurance can alleviate the burden.

Third-Party Liability

This type of cover is crucial for supply chain attacks. It provides coverage for customers and suppliers if an attack impacts them as a result of an attack on your organisation.

This is also useful if your organisation is a victim of a supply chain attack; having protection is incredibly useful if you are impacted as a result of another organisation's breach.

Business Continuity

Many cyber attacks can severely disrupt business operations, leading to the loss of data, system restoration and revenue losses during downtime. Having cyber insurance can speed up the recovery process, providing financial support that the organisation might struggle to provide after a successful attack. This will facilitate a quicker return to normal business operations.

Incident Response

Many insurers offer expert panels, which, in cases such as a ransomware attack, can provide important advice on how to handle the response. These experts can help assess the cost-benefit analysis of paying a ransom in a ransomware attack compared to rebuilding from backups etc. This can reduce the amount of downtime and improve business continuity.

Strengthen Your Supply Chain Security With ACDS

At ACDS, we firmly believe that the most efficient way to defend against evolving cyber threats is to prioritise supply chain security. Regardless of how protected you are as an organisation, if your suppliers do not have sufficient measures in place, they can be the weak link in your chain.

File Guard

ACDS' File Guard mitigates the risk of malware hidden in email attachments. Malicious attachments can lead to devastating consequences, including the deployment of malware, such as ransomware.

Ransomware can be catastrophic for organisations and their suppliers, halting operations and severely impacting customer and supplier relationships.

With File Guard, employees can open documents confidently, as the original document will be removed from the email and replaced with a new copy that has been stripped from any possible malware.

Email Guard

Email Guard protects your organisation against email fraud by ensuring that your organisation is compliant with the latest standards in email encryption and authentication.

This tool continuously assesses email security compliance and monitors the organisation's email authentication. Email Guard reduces the likelihood of spoofing, which is where attackers impersonate trusted individuals or organisations.

By bundling these products as '**Email Security Essentials**', ACDS aims to provide your organisation's suppliers comprehensive protection against supply chain attacks. It is essential to emphasise that to achieve the highest level of protection, these measures should be implemented across the entire supply chain.

Supply Chain Cyber Security FAQs

If you still have questions about how to secure your supply chain, here are some FAQs; if your question is still unanswered, do not hesitate to contact us at any time!

Why is cyber security important in the supply chain?

Cyber security plays a vital role in the supply chain as it provides protection for not only your own organisation but also your suppliers. The strength of the entire supply chain relies on the collective security measures of each organisation. You are only as strong as your weakest link; ensuring every supplier has a sufficient level of security is essential to strengthen the entire supply chain.

What are examples of supply chain cyber attacks?

Examples of recent supply chain attacks include; MoveIT, 2023, Dependency Confusion, 2021 and SolarWinds, 2020.

How to carry out a supply chain security assessment

A supply chain assessment can be carried out using these 5 steps:

1. Create a list of critical assets and key vendors/suppliers
2. For each asset and vendor, review the data housed in each and the risks
3. Request All Current and Future Suppliers Complete Self-Assessment
4. Establish a regular cadence for audits of the data stored and processed in your assets and by your vendors
5. Write an incident response plan covering your vendors and practice it

Does supply chain security impact GDPR?

Supply chain security can have a significant impact on GDPR compliance. Under GDPR, both data controllers and data processors are responsible for ensuring data protection.

When an organisation uses third-party vendors to process their data, a meticulous assessment of their security standards is conducted to ensure compliance with GDPR requirements.

If a data breach was to occur, the organisation must notify data protection authorities and individuals that have been affected within a certain time period since the initial data breach.

Secure your company today and save more time and money tomorrow

Questions?
Contact us.

acdsglobal.com

hello@acdsglobal.com

+44 3302 022 033

ACDS
ADVANCED CYBER DEFENCE SYSTEMS