From factory floor to firewall: tackling automotive supply chain risk

Net-Defence
Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 SES
Tel: 03300 241 666 • Web: net-defence.com

Over the past two to three years, supply chain (SC) risk in the automotive sector has evolved from an emerging concern to a current risk.

Today's supply chains are increasingly vulnerable, facing a wide range of threats, including economic uncertainty, political instability, natural disasters, and supplier failures, all of which can significantly disrupt operations and resilience.

In this article, however, we're focusing on one particularly urgent threat: cyber risk within your supply chain.

Most organisations rely heavily on suppliers to deliver products, systems, and services. This dependence means that a cyber attack targeting any part of the supply chain can be just as disruptive and damaging as a direct attack on your business.

As supply chains grow more interconnected and technologically advanced, the risks increase.

Take, for example, a modern car. It contains more than 100 million lines of code and around 30,000 individual components, most of which are sourced from third-party suppliers. Each of these elements represents a potential entry point for cyber criminals.

Identifying these risks can be challenging, as supply chains are often large and complex, making it difficult to pinpoint where vulnerabilities lie.

Threats can emerge at any stage and take many forms. Some are inherent to the structure of the supply chain, others may be unintentionally introduced, and some are deliberately exploited by cyber criminals actively seeking weak points to breach.

Why is the UK automotive sector a target

The UK automotive industry contributes significantly to the national economy, generating £93 billion in revenue and contributing £22 billion to UK GVA in 2024, according to the SMMT.

It invests approximately £4 billion per year in research and development and employs over 198,000 people in manufacturing, with an additional 813,000 working in the broader industry.

The sector also accounts for 12% of the UK's total export goods, generating £47 billion in trade, making it not only economically vital but also an attractive and lucrative target for cyber threats.

The risks facing the sector are increasing, particularly as manufacturing embraces digital transformation and smart factory technologies.

When you take a closer look at the UK business landscape, it becomes clear why the automotive supply chain is particularly vulnerable.

Around 99.9% of UK businesses are small and medium enterprises (SMEs), and as of early 2024, government figures show that 99.2% of those SMEs were small businesses with fewer than 50 employees.

This matters because many small businesses often serve as key suppliers within the automotive supply chain, providing essential components, services, or support. However, they often lack the dedicated cyber security expertise, processes, and financial resources needed to defend against increasingly sophisticated cyber threats.

Many operate with limited IT support, minimal formal risk management, and rely on outdated systems, making them easier targets for attackers.

Given the economic importance of the UK automotive sector, its high level of interconnectivity, and its reliance on SMEs as key suppliers, it's clear that supply chain resilience is now a cyber security priority.

Understanding your supply chain risk

Before you can start to understand the risk, you need rank the types of manufacturing suppliers you work with.

At the top of the chain are Tier 1 suppliers, those who supply directly to OEMs. These include companies providing critical components such as engines, electronic control units (ECUs), infotainment systems, and safety systems.

Next are Tier 2 suppliers, who support the Tier 1 suppliers. This group typically includes manufacturers of printed circuit boards (PCBs), producers of cable harnesses, and developers of software components that feed into larger systems.

At the base are your Tier 3 suppliers, responsible for raw materials and base components. These are the semiconductor fabrication plants, metal foundries, and chemical suppliers whose outputs underpin the entire manufacturing process.

Alongside the suppliers directly involved in automotive manufacturing, you will also work closely with a range of operational support suppliers.

These include providers of IT infrastructure, logistics and distribution services, specialist software and technology solutions, consulting and advisory firms, and technical support specialists.

This combination of production and support partners makes the automotive supply chain one of the most complex and interconnected.

What are the risks?

Here are some of the primary threats your business should be aware of:

Cyber security risk

The potential for financial loss, operational disruption, and reputational damage is significant in the automotive sector, where unauthorised access to systems and sensitive data, such as design files, production schedules, or supplier information can have far-reaching consequences.

We explored these risks in more detail during our webinar with the North East Automotive Alliance.

Operational risk

The risk of downtime or disruption to manufacturing operations caused by delays or failures in delivering critical components and parts from the wider automotive supply chain ecosystem.

Such disruptions can halt production lines, impact customer deliveries, and result in significant financial and reputational costs.

Compliance and data protection risk

IP and prototype leakage, GDPR noncompliance, and the loss of trade secrets all pose serious risks.

Cyber criminals exposing confidential designs, pre-production prototypes, or proprietary manufacturing processes can

undermine competitive advantage, loss of client trust and compromise long-term business growth.

Types of risk

There are three primary types of risk to consider:

Inherent risk

This is a vulnerability that exists within your supply chain regardless of any internal measures you put in place. Even with strong security practices in your own organisation, certain risks remain outside your direct control.

Examples include:

- Dependency on your vendors and suppliers to maintain their own security standards and deliver critical products or services.
- A lack of visibility and control over the wider supply chain network, which can make it difficult to detect or respond to emerging threats.

Introduced risk

As the title indicates, this risk is introduced into your supply chain through various factors, including human error, negligence, or deliberate malicious actions. These threats can originate from both internal personnel and external parties such as suppliers, contractors, or threat actors.

Examples include:

- Unsecure data sharing practices that expose sensitive information to unauthorised access.
- Insufficient security measures that leave critical systems or processes vulnerable to exploitation.
- The use of compromised or counterfeit components and products that can undermine the integrity and reliability of your operations.
- Failure to perform adequate due diligence when onboarding new suppliers or partners, increasing the likelihood of hidden risks entering the supply chain.

Exploited risk

This is an instance where a vulnerability is taken advantage of to launch a cyber attack or to compromise the confidentiality, integrity, or availability of business-critical systems or data. These incidents can stem from a range of causes, including technical flaws, human error, or deliberate malicious actions.

Examples include:

- Your supplier's infrastructure is used to indirectly attack your systems and data, typically through email-based methods such as phishing or malware delivery.
- Unauthorised access to your systems and data that the supplier hosts or manages on your behalf, made possible through stolen, weak, or otherwise compromised login credentials.
- Insider threat, where an employee or a supplier takes deliberate action to compromise your systems and data, often collaborating with external attackers or motivated by personal gain.

Real life examples

Some high-profile cyber attacks in recent years include:

Nissan Australia and New Zealand
Between late 2023 and early 2024, Nissan Australia and New Zealand experienced a significant cyber attack that involved unauthorised access to their local IT servers.

The breach raised concerns over data security and operational resilience, with investigations launched to determine the extent of the compromise and whether sensitive customer or business data had been accessed.

Toyota
In February 2022, Toyota was forced to suspend operations at 14 manufacturing plants across Japan after a significant cyber attack targeted one of its key suppliers.

The attack disrupted the supplier's ability to communicate with Toyota, leading to a complete halt in production for at least one day and highlighting the vulnerabilities within complex global supply chains.

Arnold Clarke
Although not a car manufacturer, on 23 December 2023, Arnold Clark fell victim to a ransomware attack. Around 5–10% of their data was encrypted before the company took the decision to shut down their systems to prevent further spread.

As a result, none of their core systems were operational following the Christmas period, disrupting key services such as new car deliveries, servicing, MOTs, and rentals. While the company stated it did not pay the ransom, the attack still resulted in an estimated £50 million in losses and took several months to fully restore operations.

CDK Global
In June 2024, CDK Global, a major provider of IT and software solutions to the automotive industry, was hit by two separate ransomware attacks in quick succession. The incidents caused widespread disruption, impacting thousands of car dealerships across North America by taking down key systems used for sales, service, and customer management.

Operations remained offline for approximately two weeks, severely affecting day-to-day business for dealerships reliant on CDK's platform. It is estimated that the financial losses from the attacks could exceed $1 billion. While CDK has not confirmed this publicly, reports suggest that a $25 million ransom may have been paid to the attackers.

How to effectively manage your supply chain

Supply chain risk management is your ally in the fight against cyber threats. Ultimately, you're looking for reassurance that your suppliers take cyber security as seriously as you do. You already carry out financial and health & safety checks, but are you checking their cyber credentials?

One effective way to gain this assurance is by verifying that they hold recognised accreditations, such as Cyber Essentials, ISO 27001, or TISAX.

Cyber Essentials

The Cyber Essentials certification scheme is designed to help protect your business against the most common cyber threats, while promoting best practices across your entire IT infrastructure.

Although most cyber attacks are relatively simple in nature, the threat landscape is constantly evolving. New risks emerge

regularly, each aiming to exploit weaknesses in your systems. By achieving and maintaining your Cyber Essentials certification, you significantly reduce your risk exposure and help protect your people, processes, customers, and finances.

For enhanced assurance, Cyber Essentials Plus (CE+) goes a step further by including an independent assessment of your systems, providing additional confidence that your defences are working effectively in practice.

What does Cyber Essential cover?

Cyber Essentials is a government-backed certification that focuses on the fundamental technical control's organisations should have in place to protect against the most common cyber threats. It's designed to help businesses of all sizes strengthen their cyber defences by addressing five key areas: firewalls, secure configuration, user access control, malware protection, and patch management.

By completing a self-assessment questionnaire, businesses can demonstrate a proactive approach to cyber security risk management. Certification shows that you are taking essential steps to safeguard your systems, data, and reputation.

In addition, UK organisations with a turnover of less than £20 million may also benefit from automatic eligibility for Cyber Liability Insurance upon achieving certification, adding an extra layer of protection and reassurance.

What does Cyber Essentials Plus cover?

Cyber Essentials Plus (CE+) builds on the core Cyber Essentials certification by including a hands-on technical verification. A certified CE+ assessor will carry out an in-depth audit of your systems, either on-site or remotely, to validate that the controls you've implemented are not only in place but also functioning effectively.

Throughout the process, we work collaboratively with you to highlight any areas that require improvement, supporting you every step of the way to meet the standard.

Achieving CE+ goes beyond ticking a compliance box, it's a clear signal to your employees, customers, and stakeholders that you are serious about cyber security and committed to upholding robust Information Security Standards.

ISO27001

ISO 27001 is the internationally recognised standard for Information Security Management Systems (ISMS). Its scope encompasses your organisation's IT systems, data, processes, and people, providing a structured framework to manage and protect sensitive information.

In simple terms, ISO 27001 acts as a blueprint for building a robust, reliable, and scalable information security management system.

By achieving certification, you not only strengthen your data protection efforts but also demonstrate your commitment to managing risk and safeguarding information, both internally and to external stakeholders.

The standard covers key areas such as:

Risk management
ISO 27001 helps you to identify, assess, and manage information security risks in a structured and systematic way, ensuring that potential threats are recognised early and addressed with appropriate controls.

CIA Triad

At the heart of ISO 27001 are three core principles of information security, confidentiality, integrity, and availability, often referred to as the CIA triad.

Together, these form the foundation for protecting your organisation's data and systems.

- **Confidentiality:** Ensuring that sensitive systems and data are protected from unauthorised access, so that only those with the appropriate permissions can view or handle them.
- **Integrity:** Safeguarding your data against unauthorised alterations, whether accidental or malicious.
- **Availability:** Making sure that your systems, services, and data are accessible to authorised employees whenever they are needed.

Data protection

While ISO 27001 is not specifically focused on personal data, it applies to all types of information, ensuring that data, regardless of its nature, is appropriately protected throughout your organisation.

It can help you strengthen your overall data governance and demonstrate a strong commitment to data protection.

Continuous improvement

Nothing stands still in the world of information security, and ISO 27001 reflects this by placing continuous improvement at the core of its certification process.

This means organisations are encouraged to regularly review and enhance their security measures to adapt to evolving threats, ensuring their systems remain resilient over time.

TISAX

TISAX is the information security standard developed specifically by the automotive industry, for the automotive industry. Originally introduced in 2017, the Trusted Information Security Exchange was established in response to the growing complexity and interconnectivity within the automotive supply chain.

It is based on the VDA ISA (the German Association of the Automotive Industry's Information Security Assessment) and is closely aligned with ISO 27001.

It includes additional controls to address key industry-specific risks such as data protection, prototype protection, third-party risk, and availability.

TISAX provides a standardised approach, where both OEMs (original equipment manufacturers) and suppliers use a common framework to assess and communicate risk. It is designed to be scalable, suppliers need only complete one assessment, which is recognised and accepted by all participating OEMs

The process of gaining the TISAX certification includes:

Identifying scope

The first step in preparing for TISAX is to define the scope of the assessment. This includes identifying which sites, processes, and assessment levels are relevant.

A clearly defined scope ensures the organisation is focused on what matters most, helping to streamline the process and reduce unnecessary complexity.

Building an internal ISMS
Once the scope is established, organisations should develop an internal Information Security Management System (ISMS).

Where possible, this should leverage existing structures based on ISO 27001, which shares a similar risk-based approach. A strong ISMS provides the framework for managing information security risks, controls, and continuous improvement in line with TISAX requirements.

Engaging an accredited audit provider
With the ISMS in place, the next step is to engage with an accredited TISAX audit provider. This external party will conduct an assessment based on the organisation's defined scope and implemented controls.

Choosing a recognised audit partner ensures that the results are valid and accepted by OEMs and other TISAX participants.

Sharing results via the TISAX platform
After the audit is complete, organisations can share their results through the TISAX platform. This enables controlled transparency, allowing OEMs and business partners to access the relevant assessment outcomes.

The centralised platform promotes a standardised, trusted exchange of security information across the supply chain.

Common pain points
Despite the clear process, many organisations encounter challenges along the way:

Readiness gaps are particularly common among smaller Tier-2 and Tier-3 suppliers, where there is often a disconnect between existing skills, knowledge, and the capacity to implement effective controls.

Cultural change can be a major hurdle. TISAX is not simply a checklist or an 'IT issue', it requires buy-in across the entire organisation, from leadership to operational teams. It's about embedding a security-conscious culture.

Managing cost versus risk is another frequent concern. Many suppliers, especially those with limited resources, struggle to balance the financial investment in TISAX readiness against the perceived or immediate business risks.

How to manage risk if your suppliers don't hold these certifications?

If some of your suppliers don't yet meet your cyber security standards or hold recognised certifications, it's important to take proactive steps to manage the associated risks effectively.

Here are some practical tips for supply chain cyber risk management in these cases:

- **Understand your supply chain:** Not all suppliers are equal. Take time to map out your supply chain and understand the role each supplier plays, especially in terms of access to sensitive systems or data.
- **Rank your suppliers:** Prioritise suppliers based on the criticality of the services they provide and the level of access they have to your systems and information. This will help focus your efforts where the risk is highest.
- **Include cyber security in your contracting process:** Make cyber security a formal part of your procurement and contracting procedures, not an afterthought.
- **Set minimum cyber security requirements:** Define clear, justified, and achievable baseline requirements that all suppliers must meet, appropriate to their level of risk.
- **Complete due diligence:** Before engaging a new supplier, ensure you assess their security posture and understand any potential risks they may introduce.

- **Request evidence:** Ask suppliers to provide documentation or proof of their cyber security practices and certifications, to verify their commitments.
- **Perform regular reviews:** Supplier risk is not static. Reassess and review suppliers on a regular basis, as their risk profile or your exposure to them may change over time.

When assessing supply chain risk, it's important to consider not only who supplies you, but also who you supply and the contractual obligations you have in place. Your risk exposure extends in both directions.

Managing risk: acceptance, mitigation or transfer

When it comes to managing risk, there are only three strategic options: accept it, mitigate it, or transfer it.

Risk mitigation can be achieved through recognised frameworks and certifications such as Cyber Essentials, ISO 27001, and TISAX.

If you're looking to transfer risk, the only viable route is cyber insurance.

Cyber insurance helps manage the financial consequences of cyber incidents by covering costs such as data breach notifications, legal fees, and business interruption losses.

Over recent years, the cyber insurance market has undergone significant changes. It has become more accessible to a wider range of businesses, thanks to the growing number of providers entering the market.

How to ensure compliance

At Net-Defence, we understand that managing cyber security compliance and reducing risk within the automotive sector can be complex and time-consuming. That's why we offer expert guidance and tailored solutions to help your organisation achieve certifications such as Cyber Essentials and maintain compliance with key industry standards.

To support this, we work closely with Hi-Comply, a leading compliance management software provider. Hi-Comply's platform is designed to automate and fast-track compliance, reduce risk, and give your business a competitive edge. Their solution supports critical certifications such as ISO 27001 and TISAX, enabling you to simplify the certification process while strengthening your security controls.

Contact our team today to learn more about managing cyber risk in the automotive sector or to get expert support with gaining these certifications.