scaut

Supply chains

Can you risk knowing nothing about the people in your supply chains?

Is there strange activity going on with your remote IT workers? What do you know about the people employed by the 3rd parties you work with? Not only is it best practice to ensure your staff are safely vetted, but also your contractors, business partners, and all the companies that make up your supply chains.

Are you protected from these risks?

Security Threats

Without proper background checks, employees with criminal records or affiliations with malicious entities might infiltrate the supply chain. This can lead to theft, sabotage, and unauthorized access to sensitive information.

Operational Disruptions

In critical supply chain operations, like those involving perishable goods or just-in-time manufacturing, even minor disruptions can impact the entire supply chain.

Regulatory Violations

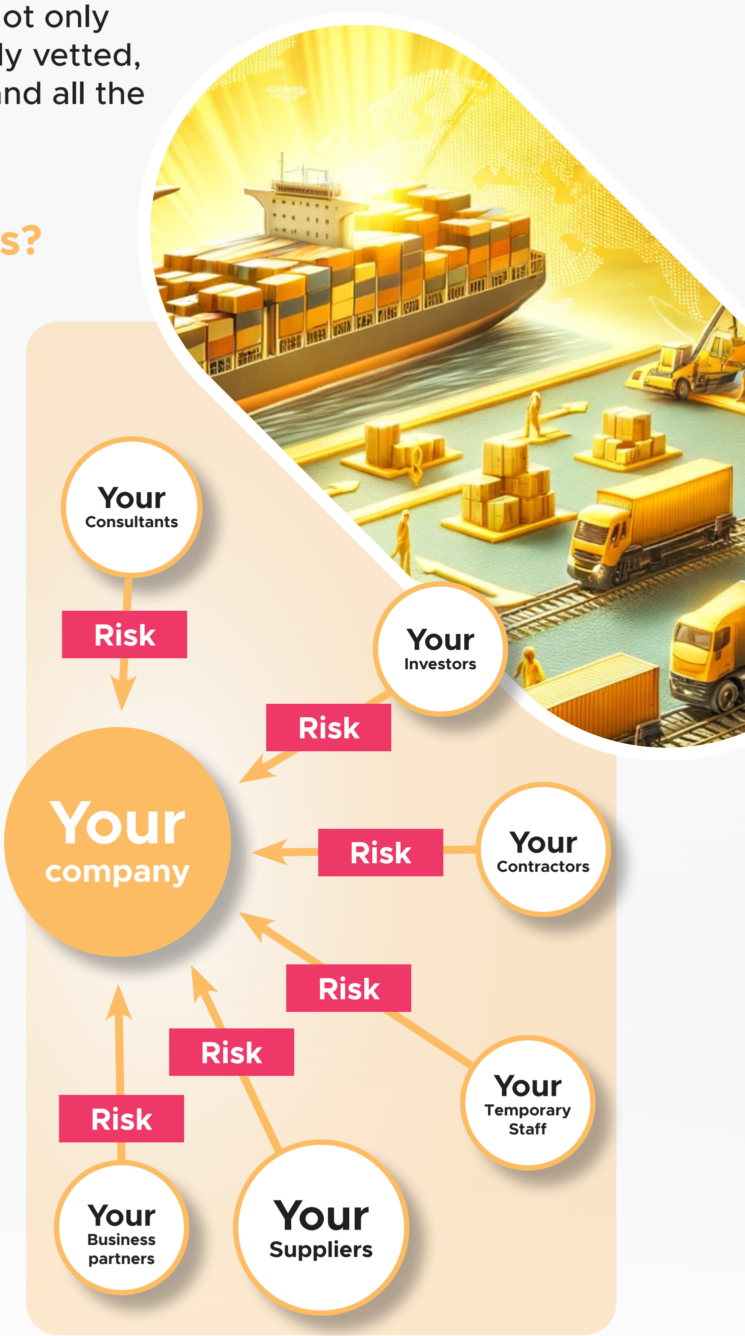
Employing individuals without the proper work authorization or those with a history of regulatory breaches can expose a company to significant legal risks.

Insider Threats

Employees with malicious intent can exploit their access credentials to cause harm. This could involve leaking confidential data, manipulating processes for personal gain, or collaborating with competitors.

Reputational Damage

Whether it's a data breach, product recall, or regulatory fine, the fallout from employing unvetted personnel can be long-lasting and detrimental to the company's public image.



You should insist on a screening process for all the personnel in your supply chain. This includes background checks, and continuous monitoring. **Talk to Scaut today.**

scaut.com

Case Study: 2024 Incident

In early 2024, a global leader in biotech with offices in the Czech Republic learned of an IT developer working under a false identity on a sensitive project.

Employed by a body-shopping agency, paid through an EoR startup Ruul in crypto, this individual had access to sensitive documents and systems for eight months before being detected. Such incidents highlight the critical need for rigorous background checks to prevent fraud and ensure the safety of company assets.

Reflecting New Regulatory Requirements

With the introduction of new regulatory frameworks such as the Network and Information Systems Directive (NIS2), the Critical Entities Resilience (CER) directive, and local laws, such as the German Supply Chain Due Diligence Act, it is imperative for companies to integrate these requirements into their tender and vendor selection processes. These regulations emphasize the need for enhanced security measures, continuous risk assessment, and stringent due diligence practices.

Ensuring that vendors comply with these standards not only helps in mitigating risks but also ensures legal compliance and promotes resilience in supply chains. Including clauses that mandate adherence to these regulatory requirements in contracts and vendor assessments will significantly bolster your company's defense against potential security threats and operational disruptions.

The cost of unsecured outsourcing

The greater the value and efficiency of your supply chain, the greater the need to protect it from the potential risks, the repercussions are many:

- Loss of contracts with clients
- Regulatory fines
- Theft of data / intellectual property
- Criminal liability
- GDPR fines

Background checks help prevent supply chain fraud.

Supply chain checklist

Before engaging with a third party, ensure the following steps are taken:

□ **Verify Business Legitimacy:** Confirm that the third-party company is registered and reputable.

□ **Conduct Comprehensive Background Checks:** Require your providers to screen all key personnel for criminal records, financial risks, and other factors.

□ **Check Work Authorization:** Ensure all employees have the legal right to work in the country.

□ **Monitor for Continuous Compliance:** Implement ongoing monitoring to catch any changes in status or behavior.

□ **Assess Cybersecurity Measures:** Verify that third-party companies have robust cybersecurity protocols in place.

□ **Evaluate Financial Stability:** Check the financial health of third-party companies to prevent disruptions due to financial failure.

□ **Review Regulatory Compliance:** Ensure that all third parties comply with relevant industry regulations and standards.

□ **Implement Regular Audits:** Schedule regular audits to maintain high standards and identify potential issues early.