Cyber and Fraud Centre Scotland

A Practical Guide to Securing Your Supply Chain

Cyber and Fraud Centre - Scotland

cyberfraudcentre.com

Contents

Topic	Page
How to secure your supply chain with simple, practical steps	Page 3
Know who you rely on	Page 4
Ask better questions before and during contracts	Page 4
Limit access and define least privilege	Page 5
Put it in writing	Page 5
Monitor and review	Page 6
Prepare for the ‘What If’	Page 6
Don’t forget people	Page 7
Quick checklist	Page 7
Making the most of our community membership	Page 8
Other resources	Page 9

How to secure your supply chain with simple, practical steps

Most cyber security incidents don't start with you. They start with someone you trust.

This could be:

- An IT provider with remote access.
- A software supplier with a vulnerability.
- A partner handling your data, be it customer or financial.

According to the UK Government's Cyber Security Breaches Survey 2025/26, 43% of UK businesses and 28% of charities reported experiencing a cyber security breach, or attack in the previous 12 month
Source - GOV.UK

Supply chain risk is now one of the biggest blind sports for organisations, because it sits outside direct control.

In this short guide, we outline areas you should focus on, to secure your supply chain. However, each supply chain is different, and you should adapt this guide to suit the needs of your organisation.

1. Know who you rely on

You can't secure what you haven't mapped.

Start by listing:

- Key suppliers - IT, payroll, cloud, tools.
- What access they have - systems, data, networks.
- What would happen if they were compromised.

Focus first on suppliers that could significantly disrupt operations across sensitive data, or affect customer trust if compromised.

The National Cyber Security Centre (NCSC) has warned of a 'significant increase' in cyber attacks resulting from vulnerabilities within supply chains in recent years
Source - National Cyber Security Centre (NCSC)

2. Ask better questions before and during contracts

You don't need a 50-page security audit. Keep it simple.

Ask suppliers:

- Do you have Cyber Essentials or Cyber Essentials Plus? This can be a useful baseline indication that a supplier has implemented fundamental security controls.
- How do you protect customer data?
- What happens if you have a breach?
- Do you use subcontractors?

If they can't answer clearly, that's a red flag.

REMEMBER
Supply chain risk isn't just physical suppliers, it also includes software providers, cloud platforms and outsourced services.

3. Limit access and define least privilege

Suppliers often have more access than they need.

Check:

- Do they have admin access when they don't need it?
- Is access always on, or only when required?
- Are accounts shared?

Reduce access to only what's necessary and review it regularly.



Supply chain attacks are particularly effective because suppliers often have trusted access to systems, services and data - making malicious activity harder to detect

Source - National Cyber Security Centre (NCSC)

4. Put it in writing

Good intentions don't protect your organisation. Contracts do.

Include:

- Security expectations.
- Incident reporting timelines.
- Data handling requirements.
- Right to review or audit, even at a basic level.

This doesn't need to be complicated. Just clear.

5. Monitor and review

Risk changes over time.

Set a simple procedure:

- Annual supplier review.
- Check for major changes (ownership, systems, breaches).
- Remove suppliers you no longer use.

Dormant accounts and forgotten suppliers are a common risk.

Following the 2025 cyber attack on Jaguar Land Rover, reports suggested disruption extended across more than 5,000 UK organisations within its wider supply chain
Source - IT Pro

6. Prepare for the 'What If'

Assume a supplier will have an incident at some point.

Ask yourself:

- Would we know?
- Who do we contact?
- Can we still operate?

Build suppliers into your incident response plan.

7. Don’t forget people

Your team interacts with suppliers every day.

Make sure they:

- Verify unusual requests (especially payment changes).
- Know who your key suppliers are.
- Flag anything suspicious and ensure everyone knows who and how to flag a potential issue.

Many supply chain attacks start with phishing or social engineering.

Breaches are expensive and disruptive

IBM’s 2025 Cost of a Data Breach Report found the global average cost of a data breach was approximately $4.44 million
Source - IBM

8. Quick checklist

- Identify your critical suppliers.
- Check their basic security posture.
- Limit and review access.
- Include security in contracts.
- Review annually.
- Plan for incidents.

Remember, you don’t need perfection, but do need visibility and controls.

Small steps make a big difference.

More about our community membership

A Cyber and Fraud Centre – Scotland membership currently includes access to our threat intelligence bulletin alongside training, guidance and CPD-accredited shared learning opportunities.

For organisations looking to strengthen cyber resilience through better understanding, collaboration and informed decision-making, our membership offers practical, user-friendly ongoing support. And it's probably more cost effective than you think - membership of the Cyber and Fraud Centre - Scotland can cost as little as the price of two coffees a week.

Members receive monthly cyber security training sessions, a free Incident Response Template, a free Cyber Policy Document and more!

To ensure you are making the most of your membership, visit our website here to see our full list of benefits - cyberfraudcentre.com/community/membership

Turning information into resilience

Cyber resilience improves when organisations stay informed, learn from others and share responsibly.

Threat intelligence, training and testing play key roles in this process. It helps organisations understand how threats work, assess their own exposure, and make meaningful improvements before an incident occurs.

To explore all aspects of a Cyber and Fraud Centre – Scotland membership, our training, testing, threat intelligence bulletin, or how shared information can support your cyber posture, speak to our team today at membership@cyberfraudcentre.com.

Other resources

This list is not exhaustive and provides a general illustration of resources available. All supply chain advice should be reviewed according to your organisation's needs, budget and level of technical knowledge.

National Cyber Security Centre (NCSC)

- Supply chain guidance - https://www.ncsc.gov.uk/collection/supply-chain-security
- Supply chain resource collection - https://www.ncsc.gov.uk/collection/supply-chain/resources
- 12 Principles of supply chain security - https://www.ncsc.gov.uk/collection/supply-chain/guidance/12-principles
- Mapping your supply chain guidance - https://www.ncsc.gov.uk/guidance/mapping-your-supply-chain
- Supplier assurance questions - https://www.ncsc.gov.uk/guidance/supplier-assurance-questions