National Protective Security Authority

In partnership with:

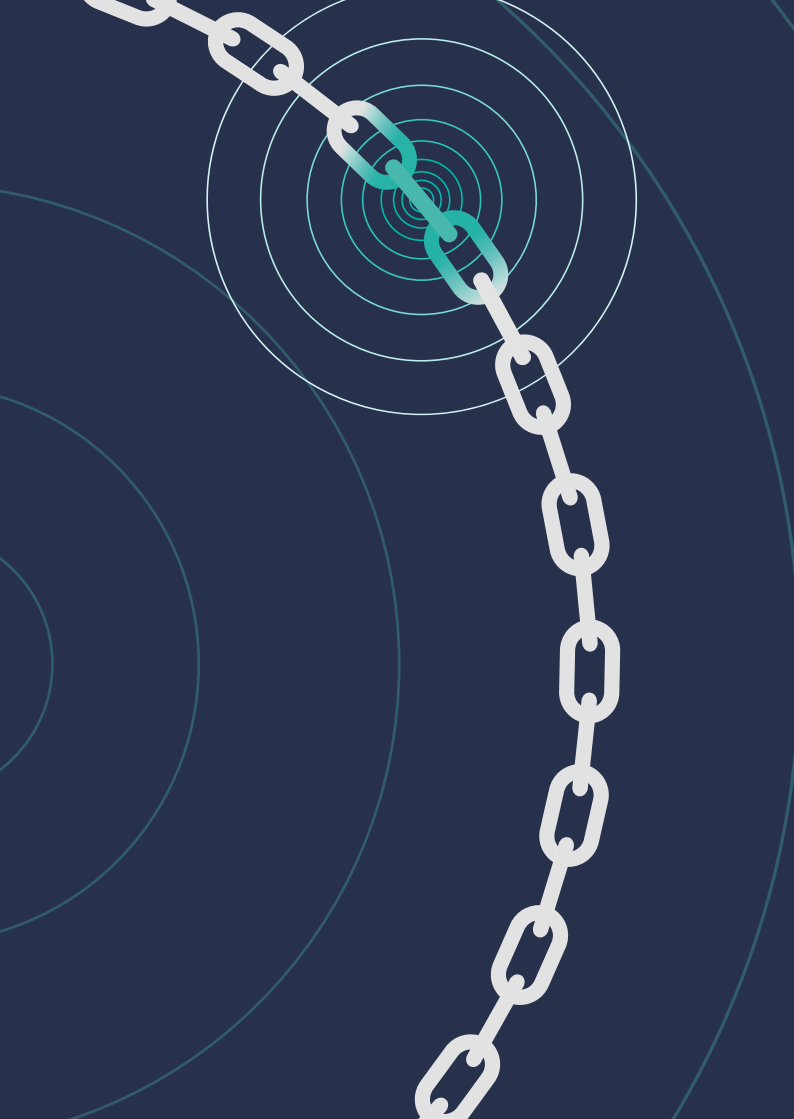
Department for Business & Trade

CIPS Chartered Institute of Procurement & Supply

PROTECTED PROCUREMENT

Supply Chain Security Guidance

BUSINESS LEADERS



CONTENTS

INTRODUCTION

Outsourcing is an essential part of business and brings with it a range of benefits. However, your supply chain also exposes you to **damaging security threats.** Attacks on your business via your supply chain happen because:

OR

Protected Procurement provides advice on how to develop your supply chain security, avoid business disruption, and protect your business.

KEY QUESTIONS

- Is supply chain security on your agenda?
- Who is responsible for supply chain security at senior leadership level?
- Do you understand your business' exposure to supply chain security threats?
- Is security embedded throughout your procurement processes?
- Do staff and suppliers understand supply chain security risks, and their responsibility to help manage them?

GOOD GOVERNANCE

Appoint a **senior leadership** lead to take responsibility for supply chain security

Integrate procurement teams into **security management processes** to defend your business from both direct and indirect attacks.

Ensure there is a **clear policy** to help staff identify and highlight high-risk suppliers and procurement activities to senior leaders.

THREATS

Ensure you know the dangers that can put your business at risk.

GEOGRAPHICAL

A supplier wittingly or unwittingly giving a foreign state access to your information or assets due to the laws to which they are bound

INSIDER

An insider attack by your supplier's employees or sub-contractors to disrupt, damage or access your assets

TECHNOLOGY

An attack on the technologies upon which you and/or your suppliers rely aiming for onward access to your systems or assets

CYBER

An attack on your supplier's IT systems aiming for onward access to your systems or assets

PHYSICAL

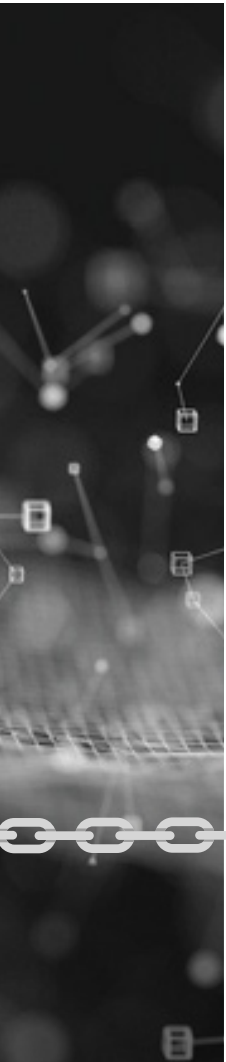
An attack on your supplier's site or during transportation designed to disrupt, damage or access your assets

HOSTILE OWNERSHIP

A supplier wittingly or unwittingly giving a foreign state access to your information or assets due to investments resulting in foreign state ownership, control or influence

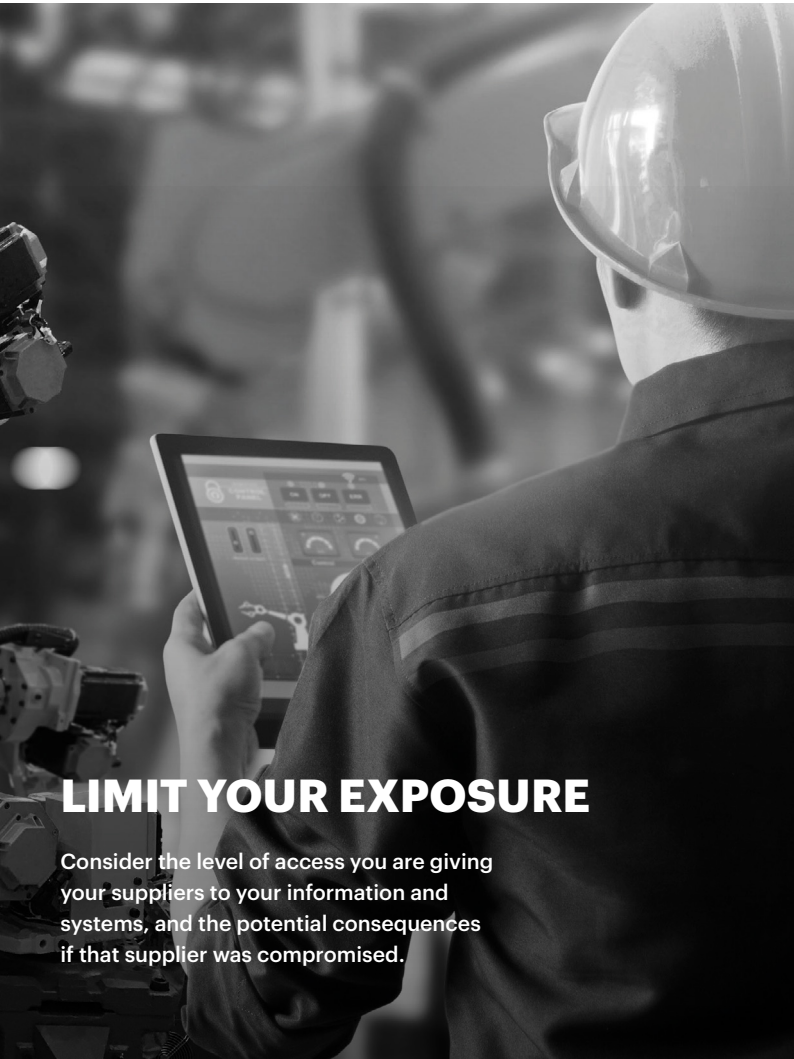
RISKS OF OFFSHORING

Offshoring parts of your supply chain may save costs or help establish a global footprint, but you cannot offshore risk or responsibility. Ensure you understand the laws by which suppliers outside the UK might be bound.



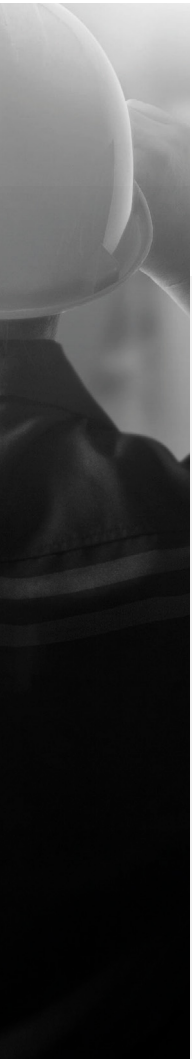
Russia has an extensive lawful intercept capability, known as the System of Operative Search Measures (SORM). SORM allows Russia's Federal Security Service (FSB), to covertly monitor communications to, within, and out of Russia. The FSB can also compel individuals and organisations to share data stored in Russia with them and could prevent the data holder from disclosing this to the data owner. All communication service providers operating in Russia are obliged to install equipment to enable the FSB to monitor communications.

China's National Intelligence Law, passed in June 2017, allows Chinese intelligence agencies to compel individuals and organisations to support and cooperate with state intelligence work. Intelligence work could capture any information collection protecting a national interest – be that military, political, economic, social, technological, cultural or others. The law does not authorise individuals or organisations to refuse to provide access, information or support if requested.



LIMIT YOUR EXPOSURE

Consider the level of access you are giving your suppliers to your information and systems, and the potential consequences if that supplier was compromised.



ELIMINATE

If a specific activity you planned to outsource provides suppliers with an unacceptable level of access to business-critical assets, **deliver the activity in-house.**

MITIGATE

If a specific activity you planned to outsource exposes more of your business-critical assets than you are comfortable with, **reduce the assets shared** to minimise your exposure.

ACCEPT

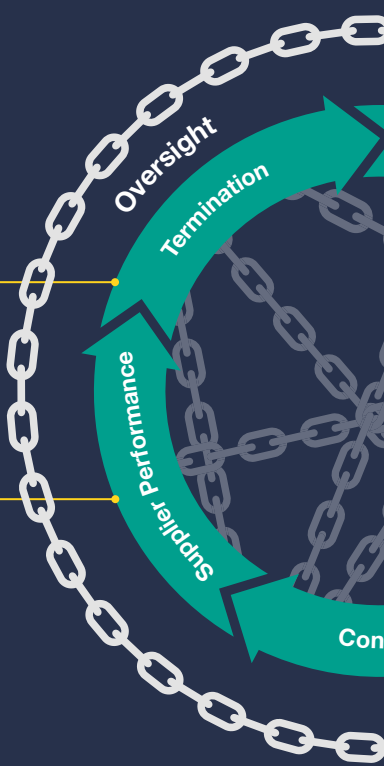
In some circumstances, businesses may find it difficult to set security expectations to suppliers that dominate the market. You should still **embed as much security as possible** across procurement processes.

Termination

Regain control of your assets from suppliers at the end of a contract.

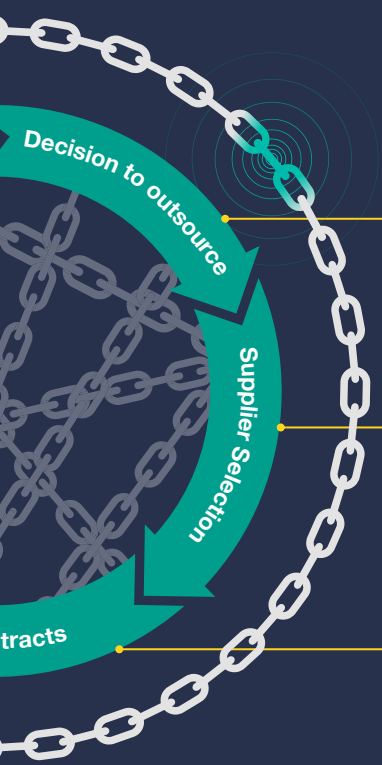
Supplier performance

Use audits and stress testing to check your suppliers' security measures are effective and meet expectations.



EMBED SECURITY WITHIN PROCUREMENT

Ensure that your procurement processes have security as a priority.



Decision to outsource

Use threat and exposure assessments to determine whether to outsource or deliver activities in-house.

Supplier selection

Assess prospective suppliers' suitability through due diligence and supplier assurance questions.

Contracts

Enforce security expectations by using appropriate security clauses in contracts.

CREATE A CULTURE OF SUPPLY CHAIN SECURITY

Lead by example, by visibly endorsing supply chain security from the top.

Support and encourage positive security behaviours across your staff and suppliers.

Ensure staff are clear about what to do if they have questions or concerns.

For more information and advice on supply chain security, visit **www.npsa.gov.uk/protected-procurement**

Disclaimer

This guide has been prepared by NPSA and is intended as general guidance only and you should not rely on it. This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness.

To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using the report. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

National Protective Security Authority

In partnership with:

Department for Business & Trade

CIPS
Chartered Institute of Procurement & Supply