CPNI
Centre for the Protection of National Infrastructure

MITIGATING SECURITY RISK IN THE NATIONAL INFRASTRUCTURE SUPPLY CHAIN

A GOOD PRACTICE GUIDE FOR EMPLOYERS

April 2015

Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Table of contents

Executive summary

Most organisations have multi-tiered supply chains which are likely to be both upstream (supply) (i.e. between the organisation and the organisation's suppliers or suppliers' suppliers) and downstream (demand) (i.e. between the organisation and its market). Vulnerabilities in these supply chains can introduce vulnerabilities to the organisation itself and to its assets. Those vulnerabilities can expose the organisation and its assets to risk from national security threats, principally terrorism, hostile cyber-attacks by foreign states and large scale cyber-crime.

Supply chain security risk is a business risk which can only be mitigated through a holistic risk mitigation plan. This is a business risk which has to be addressed through a collaborative approach involving leadership within the business together with specialist functions such as procurement, security, IT etc. Supply chain security risk can never be outsourced to the upstream or downstream suppliers – it will always remain owned by the business. Business risks of this sort demand board oversight and the board will ultimately be responsible for failures of the organisation's supply chain security risk mitigation arrangements.

Supply chain security risk mitigation will invariably bring additional business benefits such as countering data protection or fraud risks resultant from vulnerabilities in the organisation's supply chain. While supply chain security risk mitigation arrangements are not intended to address issues of business continuity or resilience of the supply chain to hazards, it is likely that there will be business benefit in addressing all these issues in a complementary way.

The Centre for the Protection of National Infrastructure (CPNI) recommends that organisations should view supply chain security risk as being an extension of existing arrangements to mitigate security risk within the organisation itself. To achieve this extension requires a supply chain security risk mitigation implementation plan which includes:

- Comprehensive mapping of all tiers of the upstream and downstream supply chains to the level of individual contracts.
- Risk scoring each contract to link in to the organisation's existing security risk assessment.
- Due diligence/accreditation/assurance of suppliers (and potential suppliers) and the adoption, through contracts, of proportionate and appropriate measures to mitigate risk.
- Audit arrangements and compliance monitoring.
- Contract exit arrangements.

Establishing a supply chain security risk mitigation plan is a non-trivial task and requires appropriate resourcing. The investment of time, effort and money needs to be proportionate to the potential impact of the risks being mitigated. This requires a board level judgment which can only be taken if the board itself properly understands the risks in the first place. It will also be affected by the maturity of the organisation's existing approach to security risk mitigation, by the complexity of its supply chain and by the prevailing threat picture. For some organisations this will amount to reviewing and perhaps enhancing existing arrangements. For others this will be a major new area of activity to address risks which have either not previously been understood or which have been negligently ignored.

Introduction

The aim of this guidance

This guidance provides information about good practice for organisations to mitigate security risks to themselves and their assets which result from vulnerabilities in their supply chain.

Clarification of terminology and focus

A great deal of available guidance claims to address issues of supply chain security. However, in many cases this actually refers to continuity of supply and other guidance relates only to information risk. The objective of 'Mitigating security risk in the national infrastructure supply chain' is: "Mitigation of holistic security risks to national infrastructure organisations and their assets resulting from vulnerabilities in their global supply chains."

The guidance focuses on:

- **Security risks** – the National Security Risk Assessment states the Tier 1 risks to be terrorism, hostile cyber-attacks by foreign states and large scale cyber-crime. Implementation of this guidance may also be applied to other risks such as data-protection, countering fraud etc. but that is not the primary focus. Business continuity, supply chain resilience and vulnerability to hazards are not a focus of this guidance but again the outputs may be relevant to addressing those business risks.
- **National infrastructure** – as defined on the CPNI website as "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends". This guidance is therefore aimed at a wide range of organisations in terms of size and function and it is anticipated that it will also be of value to organisations beyond the national infrastructure.
- **Supply chain** – this is widely interpreted as being multi-tiered and being both upstream (supply) (i.e. between the organisation and the organisation's suppliers or suppliers' suppliers) and downstream (demand) (i.e. between the organisation and its market).
- **Assets** – most available supply chain security guidance is narrowly drawn around a specific issue, for example, information assets. This guidance applies to all of a national infrastructure organisation's assets which might be impacted by security threats. This will include physical, information and personnel assets as well as other critical business assets such as intellectual property. By extension this guidance is likely to be useful in mitigating security risks which might impact on other business assets such as reputation, brand etc.
- **The holistic approach** – security risks are interlocking: a physical security breach may be caused by a human failing or a cyber-attack; data theft may be the result of an insider attack; etc. Addressing physical, cyber and personnel security issues holistically is necessary for all security risk mitigation including supply chain security risk mitigation. (See also example scenarios on page 6.)
- **Global supply chains** – most complex supply chains (and some national infrastructure organisations themselves) are global. This guidance is set against a UK Critical National Infrastructure (CNI) background but it is intended to be applicable globally. However,

organisations will have to ensure that their supply chain security risk mitigation plan takes account of differing legislation, regulation, standards and approaches to security and culture amongst their global suppliers.

This document should be read in conjunction with other guidance published by CPNI, in particular:

- *Personnel Security Risk Assessment: a guide*
- *Holistic Management of Employee Risk (HoMER)*
- *Personnel Security and Contractors: a good practice guide for contractors*
- *Physical Security over Information Technology*

The guidance documents referred to above are available on www.cpni.gov.uk.

Supply chain security risk scenarios

Scenario 1: A national infrastructure organisation operating over a number of critical sites has outsourced its on-site catering arrangements to a single supplier. The supplier provides catering staff to all the sites and arranges the delivery of catering supplies to those sites by sub-contractors. The catering supplier has access to the organisation's IT network in order to manage catering for special events, meetings etc. Employees of the organisation pay for meals using cash credit loaded onto their staff passes, giving the catering supplier access to personal data about employees and to the access control system.

Scenario 2: A national infrastructure organisation operating over a number of critical sites has outsourced the supply, installation and maintenance of its integrated CCTV, perimeter intrusion, access control and security control room equipment to a single supplier. That supplier therefore has privileged information to the physical security arrangements of all the sites. Additionally, components of the integrated system are sub-sourced to a range of global suppliers and within those components are sub-components which are bought from further tiers of global suppliers. Vulnerabilities in any of the components or sub-components may expose the national infrastructure organisation to physical security risks.

Scenario 3: A national infrastructure organisation uses specialist systems (e.g. industrial control systems, building management systems etc.) provided by outsourced suppliers. These suppliers have continuing access to the organisation's network in order to performance monitor the specialist systems, carry out patching etc.

Scenario 4: A national infrastructure organisation operating over a number of critical sites has outsourced all its manned guarding. In order to fulfil their function, the guarding companies require unrestricted access across these critical sites.

Scenario 5: A defence/aerospace organisation produces manufactured items for supply to the UK armed forces/aviation sector. The items require sub-components from a range of global suppliers. The organisation is concerned that the sub-components might import vulnerabilities which can subsequently be exploited as attack vectors on the items. The organisation is also concerned about the ability of suppliers to deduce information about the end use of the items and hence the capability of the end user.

Scenario 6: A national infrastructure utility provider has an outsourced call centre which has access to the totality of its customer data including sensitive financial information.

First steps and governance

There is little point in embarking on a supply chain security risk mitigation programme unless the organisation already takes a sound approach to managing its internal security risks. Indeed, it is not possible to carry out such a programme unless it links back to a comprehensive organisational risk assessment. For the purposes of this guidance, therefore, it is assumed that:

- **Governance**: recognising that holistic security risks are a business risk, the board takes ownership and accountability for all aspects of security risk in the organisation.
- **Roles, responsibilities and resources**: the board has delegated roles and responsibilities for managing different aspects of security risk and ensured that the measures and procedures from the top down are clearly understood by all involved are and appropriately integrated and resourced.
- **Assets**: the organisation fully understands its critical assets and their vulnerabilities. Recognising that the criticality of assets varies with circumstances (e.g. data relating to mergers and acquisitions activities) there is a review process in place to constantly update the list of critical assets.
- **Risk**: the organisation conducts a full formal review of holistic security risks at least annually; such risks are on the top risk register and the board is fully sighted on the specific vulnerabilities which constitute the highest level of risk and on the mitigating measures in place to manage those risks; the board has proactively articulated its attitude to security risk tolerance and this is understood in the organisation.
- **Impact**: the board understands the impact (including operational, financial, reputational and legal) that a security incident would have on both the organisation and on the board itself.
- **Response**: the organisation is appropriately prepared to react in response to a security incident, to minimise harm and to maximise possibility of attribution and appropriate action with respect to the perpetrator. Response is practised through an exercise programme (including at board level).
- **Audit**: the audit committee reviews the overall management of security threats on an annual basis with particular emphasis on ensuring that risks and assets are regularly reviewed and are current and that the policies and procedures involved are functioning well, properly integrated, and compliant with legal and regulatory frameworks.

Against this background, and recognising that an organisation's security risks can never be outsourced, the board will take ownership of the decision to implement a programme to mitigate holistic security risks in the upstream and downstream supply chains.

Supply chain security risk mitigation methodology

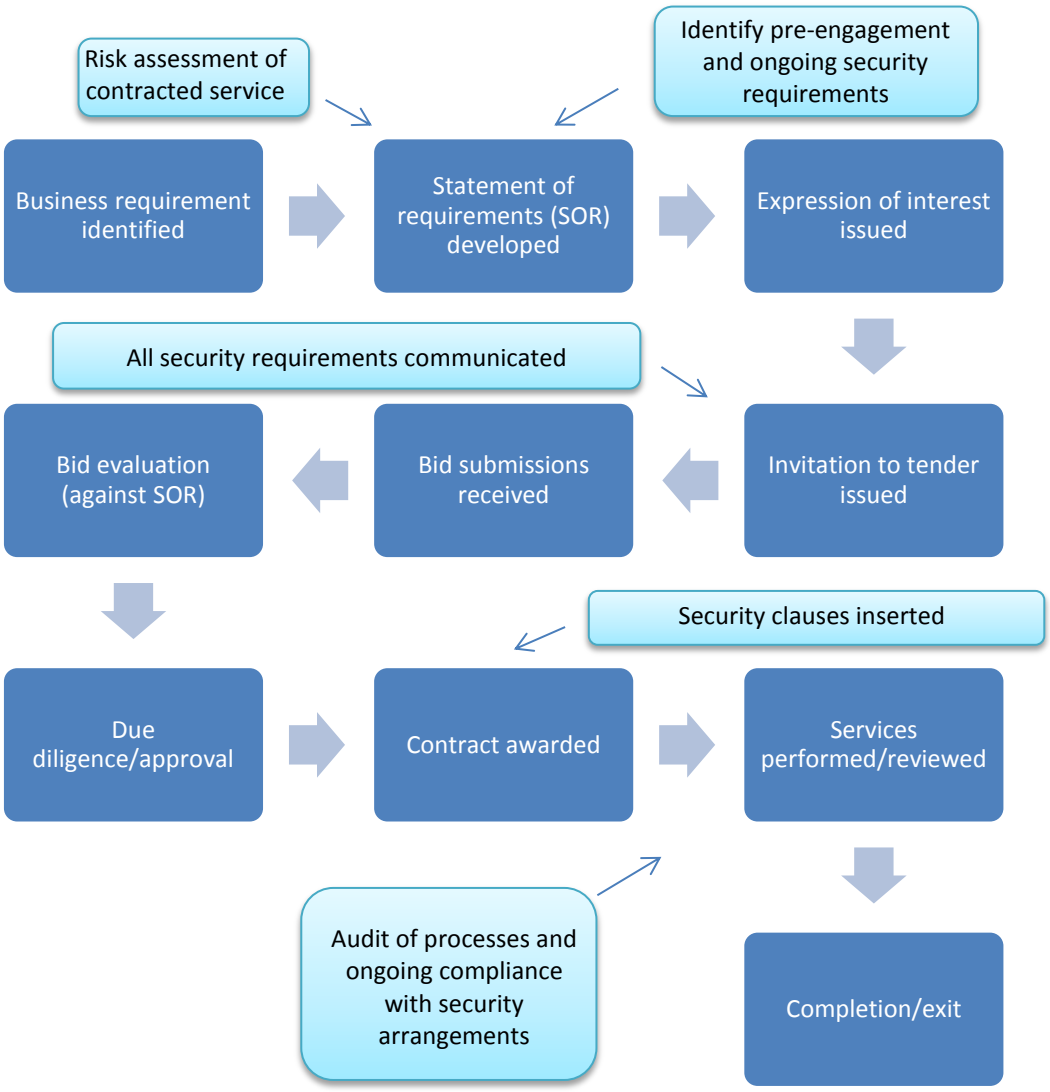
The overall methodology to implementing a supply chain security risk mitigation plan is as follows:

- Mapping the upstream and downstream supply chains in detail to the level of individual contracts and sub-contracts.

- Extending organisational risk assessment to the upstream and downstream supply chains: including scoring individual contracts and sub-contracts for risk.
- Conducting due diligence/accreditation/assurance of supplier (and potential supplier) organisations: proportionate and appropriate measures according to the risk and ranging from statements of assurance (with suggested drafts), through formal accreditation (e.g. to ISO 27001), to actual inspection of the supplier by the prime. Use of appropriate tools to manage supplier relationships.
- Applying contractual clauses to address supply chain security issues.
- Audit arrangements and compliance monitoring through the contract lifetime.
- Contract exit arrangements: Making appropriate arrangements to ensure that there is no residual risk once the contract has been completed.

The process for assessing individual contracts is shown in the following diagram:

Security in the contract cycle



Proportionate implementation of a supply chain security risk mitigation plan

The decision by the board to implement a holistic security risk mitigation plan across an organisation's global supply chain may seem daunting to those charged with taking forward the action. Clearly not everything can be done overnight and it is necessary to take a phased approach. CPNI recommends that no new contracts should be undertaken without being subjected to the security process described above.

However, for existing contracts (which may be numerous and complex) CPNI recommends a three stage approach, documenting the outcomes in a format along the lines of Annex A:

Stage 1: This stage will probably be led by the organisation's procurement team. The objective is simply to list all contracts and sub-contracts in the organisation's upstream and downstream supply chains. The information required at this stage is that listed in Columns A to F of the form at Annex A. It is assumed that this information will all be readily available to the procurement department. In the event that it is not, then the missing information will have to be obtained from the manager with responsibility for the contract and/or from the supplier. The latter may be necessary in particular with regard to sub-contracts.

Stage 2: This stage will probably be led by the security team or by the team established to implement the supply chain security risk mitigation plan. The objective is to complete Columns G and H of the form at Annex A. CPNI recommends that this work is completed through joint meetings between the managers responsible for the contracts and the security team. It is not acceptable to invite such managers to make their own assessments of risks and vulnerabilities. For example, a facilities manager with oversight of a catering contract (such as that listed in Scenario 1 on page 6) is unlikely to have sufficient understanding of security matters to make the necessary judgements. The vulnerabilities inherent in such a contract can only be unpicked through detailed dialogue between the facilities manager about how the contract functions in practice and someone with a sound overview of the organisation's assets and risk assessment.

Stage 3: This stage will probably be led by the security team or by the team established to implement the supply chain security risk mitigation plan but will additionally require the engagement of the procurement team and the manager responsible for the contract. The objective is to complete Columns I and J of the form at Annex A. In effect this will require balance judgement encompassing the priority of the risks that need mitigating, the feasibility of doing so within the terms of the existing contract (e.g. perhaps by carrying out additional compliance checks, additional screening of deliveries etc.), the possibility and cost of modifying the existing contract, and the remaining life of the contract. Outcomes may include contractual action with the supplier to mitigate risk, understanding and tolerance of risk through to the end of the contract, or simply noting the requirement for changes when the contract is re-tendered.

Organisations which already have sophisticated vendor management systems in place will wish to adapt this process to suit their own circumstances but the outcome should still be a complete understanding of the mapped security risks in the supply chain, on a supplier by supplier basis, and a prioritised action plan for mitigating the highest risks.

Additional references

In addition to CPNI documents referenced above, the following documents will also be useful to organisations developing a supply chain security risk mitigation plan:

- Cabinet Office "Supplier Assurance Framework: Good Practice Guide Version 2 – February 2015". Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/407165/Supplier_Assurance_Framework_GPG__Final_2_0.pdf
- Department of Transport and Cranfield University School of Management "Understanding Supply Chain Risk: A Self-Assessment Workbook". Available at: https://dspace.lib.cranfield.ac.uk/handle/1826/4373
- HMT "The Orange Book – Management of Risk: Principles and Concepts". This is available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf
- ISO 27001 Information technology — Security techniques — Information security management systems — Requirements: This (and the associated ISO 27002) is available at: http://shop.bsigroup.com/ProductDetail/?pid=000000000030126472
- Cyber Essentials and Cyber Essentials Plus: This is available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf
- ISO 28000 Specification for security management systems for the supply chain: This is available at: http://shop.bsigroup.com/ProductDetail/?pid=000000000030155502
- ISO 28001 Security management systems for the supply chain. Best practices for implementing supply chain security, assessments and plans. Requirements and guidance: This is available at: http://shop.bsigroup.com/ProductDetail/?pid=000000000030161532

Annex A

Supply chain security risk mapping

A	B	C	D	E	F	G	H	I	J
Serial	Name of supplier organisation	Scope of the contract	Name or appointment of manager responsible for the contract	Date contract commenced	Date contract due to terminate	Assets potentially impacted by supplier vulnerabilities and description of vulnerabilities	Existing mitigation measures and current risk rating (H,M,L)	Additional mitigation measures which could be imposed and amended risk rating (H,M,L)	Priority for action