CPNI
Centre for the Protection of National Infrastructure

Protect Your Supply Chain Resilience

PUBLISH DATE: October 2021

CLASSIFICATION: Official

Guidance for organisations during a crisis or times of significant change to enhance supply chain security and avoid disruptions being exacerbated by security incidents

Introduction

Supply chain protective security during a crisis, or times of significant change, is of vital importance. The importance or criticality of affected supply chains may rise in response to a changing economic and operational environment. This guidance aims to inform your decision making to ensure that a proportionate risk management approach is taken to support the resilience of your supply chain operation and wider supply network by addressing three overarching risks:

1. Exploitation of the changing situation by hostile adversaries.
2. Baseline protective security measures being neglected at critical nodes.
3. Failure to establish and utilise effective incident and crisis management capabilities

The Threat:

1. **Economic Leverage:** If companies in your industry or supply chain fall into financial distress, this may make them less resistant to **hostile direct investment** or other economic leverage. Hostile states may deliberately use this to access critical systems, key individuals, or sensitive intellectual property. If this is extensive across your industry, it may create a strategic dependence on that state which could be used to influence the UK in their favour.
2. **Insider Threats:** Where your staff face greater uncertainty or personal grievances, for example unexpected loss of employment or financial difficulties, this may make them more vulnerable to **financial inducements or other pressure**. A range of hostile actors – from criminals to foreign states – might exploit this vulnerability to undermine your business or gain an advantage over it.
3. **Interference:** State actors may seek to amplify public messages or seed narratives with the intent to cause alarm or which undermine the UK, your industry or company. This could be achieved through **targeted mis- or disinformation** which could exacerbate issues by prompting 'panic buying' or undermining confidence in your organisation or supply chain.

Protective security principles to raise your supply chain's resilience

1. **Anticipate and assess** the risks by reviewing your risk register in response to a changing external environment. Consider the risk of, reactively, bypassing due-diligence processes and enforcing weak contractual risk controls on new and existing suppliers.

Protective Security

2. **Maintain** protective measures proportionate to the anticipated risk at critical nodes, in the following areas:
    a. Personnel
    b. Processes
    c. Technology
    d. Information
    e. Facilities

3. **Manage Incidents** through established and practised standard operating procedures (SOPs) for risk you have identified Ensure a cross-functional team are part of the incident management team (IMT) and document your procedures. Having a protective security representation is best practice.

4. **Respond** to incidents that cannot be controlled or foreseen through the risk assessment, by establishing a crisis management capability that is integrated with the protective security function.
    a. Establish a Crisis Management Plan (CMP) overseen by a Crisis Management Team (CMT), identifying critical roles and responsibilities, functions, and communication and decision-making procedures.
    b. Conduct training and planning exercises using the CMP to stress test its effectiveness.
    c. Ensure an **effective external communication response** is included to mitigate **poor or malicious** risk communication that may impact public and stakeholder confidence.
    d. Engage with public sector bodies at the earliest opportunity during a crisis.

FAQs

Q. What is the difference between Supply Chain Resilience and Supply Chain Security?
A. Supply chain security (SCS) is protecting against the exploitation of vulnerabilities within your supply chain facilitating unauthorised access to protected or sensitive information, systems, and infrastructure. SCS is one of the defensive functions of resilience - supply chain resilience is the capability of an organisation, supply chain or supply network to anticipate, prepare and adaptively respond to changes or disruptions.

Q. Where can I get further advice about supply chain security?
A. The joint CPNI and NCSC Supply Chain Security Collection guidance describes 12 principles that should be used to help guide your supply chain security programme.

Q. Is there a framework for mitigating insider risk in my organisation?
A. CPNI's Insider Risk Mitigation Framework provides an overview and links to further guidance on insider risk management.

Q. Who should be part of my incident management team?
A. Your incident management team should be as close to the location and familiar with the operation as possible, to facilitate effective communication and teamwork. This team should also include the key functions that are necessary for the standard operating procedures (SOPs) to be implemented effectively. The aim should be to follow the SOP to contain the incident.

Q. **Who should be part of my crisis management team (CMT)?**
A. A CMT should be strategically focused with input from specialists to inform decision making. A fundamental objective of crisis management is to have good governance: having clear lines of authority and responsibility is paramount. A second fundamental objective is effective communication that is both efficient internally and effective externally, to reduce panic and manage stakeholders' expectations. A good CMT might consist of:

- A CMT Leader (with a direct line to the most senior decision maker within the organisation)
- Human Resource Leadership
- Public Relations Leadership
- Security Leadership
- Operations Leadership
- Finance Leadership
- Legal Counsel

Q. Why should external communication be part of my organisation's crisis management plan?
A. Interference from adversaries has been highlighted as a credible threat during times of crisis. The most effective countermeasure to misinformation is to ensure that external communications are both impactful and efficient.

Q. What's the difference between an incident and crisis?
A. An incident is a foreseeable risk that can be managed. If an incident isn't managed effectively or isn't anticipated, it has a high likelihood of becoming a crisis. A poorly managed crisis has a high likelihood of becoming a disaster.

Q. Why does CMT and IMT need different structures?
A. In some organisations, particularly smaller organisations, the IMT may be the same as the CMT. However, the CMT should, generally, be more strategically focused with higher authority and wider responsibility. The IMT will be situation specific and require a more operational level of understanding and influence.

Q. Should my organisation heighten the due-diligence process during a crisis?
A. Your risk assessment should inform this decision. In times of crisis prospective suppliers may be strained and have unidentified risks. Developing an appropriate level of knowledge about an organisation before engaging it as a supplier, is best practice.

Q. I have a small team; how can I establish a crisis management function?
A. Even small organisations should establish a crisis management function. Having a well-informed team with the authority to make strategic decisions autonomously is a key ingredient for a successful CMT of any size.

Q. Are there any standards my organisation should be aware of?
A. There are numerous standards that may influence your supply chain security during uncertain times: BS 11200 Crisis Management, ISO 22320 Emergency Management, ISO 22320 Business Continuity Management, ISO 28000 Supply Chain Security Management Systems.

Q. Can you describe criticality as it applies to supply chains?
A. A useful way of thinking of criticality is how important it is to the continuation of an operation or other's operation. To help judge, consider how impactful a compromise or disruption would be and how long it would take to recover a to fully functioning supply chain or operation from its loss or disruption?

Q. Why does the criticality of supply chains change during crisis?
A. Adversaries will gravitate to the most attractive and fragile target – visibility of further networks that will be impacted by a successful attack and vulnerabilities will be more likely to be exposed, will be revealed during a crisis. The downtime will increase due to strains on supply and demand and the impact of a successful attack will magnified.