CPNI
Centre for the Protection
of National Infrastructure

National Cyber
Security Centre

Supply chain security collection

Guidance January 2018

Proposing a series of 12 principles, designed to help you establish effective control and oversight of your supply chain. For the purposes of this paper a supply chain is ‘a network of entities connected by a series of trading relationships’.

The guidance covers cyber, physical and people security

1 **The principles of supply chain security**
This guidance proposes a series of 12 principles, designed to help you establish effective control and oversight of your supply chain.

2 **I. Understand the risks**
The first three principles deal with the information gathering stage.

3 **II. Establish control**
This section’s principles will help you gain and maintain control of your supply chain.

4 **III. Check your arrangements**
Businesses will need to gain confidence in their approach to establishing control over their supply chain.

5 **IV. Continuous improvement**
As your supply chain evolves, you’ll need to continue improving and maintaining security.

6 **Example supply chain attacks**
A selection of illustrative real-world examples of supply chain attacks.

7 **Assessing supply chain security**
The table below gives you a series of scenarios against which to measure the security of your supply chain.

8 **Assessing supply chain management practice**
It is expected that your will already be following good procurement and contracting practice. This guidance offers additional factors that you may consider.

9 **Supply chain security: 12 Principles**
The twelve principles in an abbreviated, easy to digest, printable format

1 The principles of supply chain security

This guidance proposes a series of 12 principles, designed to help you establish effective control and oversight of your supply chain.

Introduction

The guidance will provide organisations with an improved awareness of supply chain security, as well as helping to raise the baseline level of competence in this regard, through the continued adoption of good practice. Whilst beneficial, this guidance has not been written for organisations with national security (high assurance), requirements.

Most organisations rely upon suppliers to deliver products, systems, and services. You probably have a number of suppliers yourself, it's how we do business.

But, supply chains can be large and complex, involving many suppliers doing many different things. Effectively securing the supply chain can be hard because vulnerabilities can be inherent, or introduced and exploited at any point in the supply chain. A vulnerable supply chain can cause damage and disruption.

Despite these risks, many companies lose sight of their supply chains. In fact, according to the 2016 Security Breaches Survey, very few UK businesses set minimum security standards for their suppliers.

A series of high profile, very damaging attacks on companies has demonstrated that attackers have both the intent and ability to exploit vulnerabilities in supply chain security. This trend is real and growing. So, the need to act is clear.

The principles

This guidance proposes a series of 12 principles, designed to help you establish effective control and oversight of your supply chain. We have divided these principles, into four sections, each representing a stage in the process.

These are:

I. Understand the risks

Before you can do anything to secure your supply chain you need understand the risks (and benefits) you are taking on by engaging suppliers.

II. Establish control

How to gain control of your supply chain. This section includes four case studies:

1. Protecting information that you share with suppliers.
2. Specifying security requirements to a supplier who is delivering something to you.
3. Connecting a supplier's systems to yours.
4. National security case - where a state actor may target you.

III. Check your arrangements

Businesses will need to gain confidence in their approach to establishing control over their supply chain.

IV. Continuous improvement

As your supply chain evolves, you'll need to continue improving and maintaining security.

Additional content

These example supply chain attacks give further context to the principles.

A note on implementation

Implementing these recommendations will take time, but the investment will be worthwhile. It will improve your overall resilience, reduce the number of business disruptions you suffer and the damage they cause. It will also help you demonstrate compliance with GDPR, the new Data Protection Act. Ultimately, these measures may help you win new contracts, because of the trust you have sought in the security of your supply chain.

Further reading

The following sources provide information on managing supply chain security threats and risks:

DCPP (MoD) – DCPP is a joint Ministry of Defence (MOD) / industry initiative to improve the protection of the defence supply chain from the cyber threat.

Government supplier framework – This framework helps the government to manage supplier risk.

IS0 28000 – Specification for security management systems for the supply chain.

2 I. Understanding the risks

The first three principles deal with the information gathering stage.

Until you have a clear picture of you supply chain, it will be very hard to establish any meaningful control over it. You will need to invest an appropriate amount of effort and resource to achieve this.

1. Understand what needs to be protected and why

You should know:

- The sensitivity of the contracts you let or will be letting.
- The value of your information or assets which suppliers hold, will hold, have access to, or handle, as part of the contract.

Think about the level of protection you need suppliers to give to your assets and information, as well as the products or services they will deliver to you as part of the contract.

2. Know who your suppliers are and build an understanding of what their security looks like

You should know:

- Who your suppliers are. You will need to think about how far down your supply chain you need to go to gain understanding and confidence in your suppliers.

You may have to rely on your immediate suppliers to provide information about sub-contractors, and it may take some time to ascertain the full extent of your supply chain.

- The maturity and effectiveness of your suppliers' current security arrangements. For example you could use CPNI Protective Security Management Checklist to assess the maturity of your suppliers' people security arrangements.
- What security protections you have asked your immediate suppliers to provide, and what they, in turn, have asked any sub-contractors to do:
- Determine whether or not your suppliers and their sub-contractors have provided the security requirements asked of them.
- Understand what access (physical and logical) your suppliers have to your systems, premises and information and how you will control it.
- Understand how your immediate suppliers, control access to, and use of, your information and/or assets - including systems and premises, by any sub-contractors they employ.

You should focus your efforts in this area on those parts of your suppliers' business or systems that are used to handle your contract information, or to deliver the contracted product or service.

3. Understand the security risk posed by your supply chain

Assess the risks these arrangements pose to your information or assets, to the products or services to be delivered, and to the wider supply chain.

Sources of risk

Risks to and from the supply chain can take many forms. For example, a supplier may fail to adequately secure their systems, may have a malicious insider, or a supplier's members of staff may fail to properly handle or manage your information.

It could be that you have poorly communicated your security needs so the supplier does the wrong things, or the supplier may deliberately seek to undermine your systems through malicious action (this may be under state influence for national security applications).

Use the best information you can to understand these security risks. For example:

- Common cyber attacks - reducing the impact
- Insider data collection report
- Insider risk assessment
- CPNI Holistic Management of Employee Risk (HomER).

Descriptions of four known cyber attacks on supply chains (third party software providers, website builders, third party data stores and watering hole attacks) are also provided here. You should also watch out for routine threat advisories published by NCSC and CPNI.

Getting mitigation right

Understanding the risk associated with your supply chain is key to ensuring security measures and mitigations are proportionate, effective and responsive. Further information can be found at Risk Guidance - First Drop and CPNI Operational Requirements.

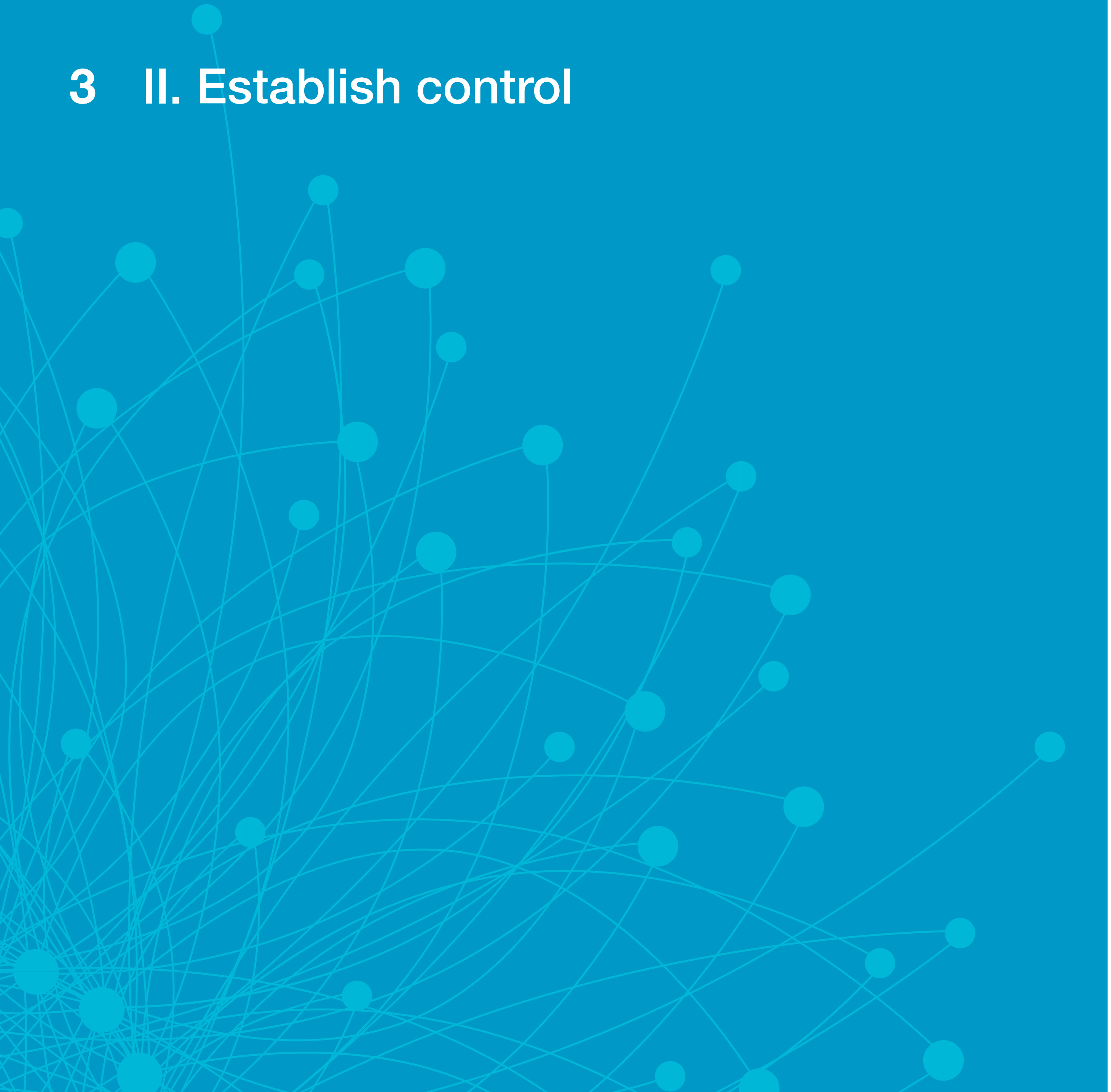
Use this understanding to decide the appropriate levels of protection you will expect suppliers across your supply chain to provide for any contract information, and contracted products or services.

Plan of action

It may be useful to group different lines of work, contracts or suppliers into different risk profiles, based on considerations such as: the impact on your operations of any loss, damage or disruption, the capability of likely threats, the nature of the service they are providing, the type and sensitivity of information they are processing etc. Each profile will require slightly different treatment and handling to reflect your view of the associated risks. This may make things easier to manage and control.

You should document these decisions and share them with suppliers. For example, you may decide that contracts which provide basic commodities such as stationery, or cleaning services require very different approaches to management to those that provide critical services or products.

3 II. Establish control



This section's principles will help you gain and maintain control of your supply chain.

Once you gain better control of your supply chain you will be able to analyse strategic risks to it.

For example to:

- Identify any suppliers who continually fail to meet your security and performance expectations.
- Identify critical assets and any over-reliance on single suppliers. This will help you to build further diversity and redundancy into your planning.

4. Communicate your view of security needs to your suppliers

Ensure that your suppliers understand their responsibility to provide appropriate protection for your contract information and contracted products and services and the implications of failing to do so.

Ensure your suppliers adhere to their security responsibilities and include any associated security requirements in any sub contracts they let.

You should decide whether you are willing to permit your suppliers to sub-contract and delegate authority to do so appropriately.

Give your suppliers clear guidance on the criteria to use for such decisions (e.g. the types of contract that they can let with little/no recourse to you, and those where your prior approval and sign-off must always be sought).

5. Set and communicate minimum security requirements for your suppliers

You should set minimum security requirements for suppliers which are justified, proportionate and achievable.

Ensure these requirements reflect your assessment of security risks, but also take account of the maturity of your suppliers' security arrangements and their ability to deliver the requirements you intend to set.

It may also be sensible to identify circumstances where it would be disproportionate to expect suppliers to meet the minimum security requirements. For example, this may only be relevant for those suppliers who only need ad hoc, or occasional access to limited and specific data, and/or access to your premises.

You should document these considerations and provide guidance on the steps you intend to take to manage these engagements. This approach could help reduce your workload and avoid creating additional, unnecessary work for these parties.

Case by case

Consider setting different protection requirements for different types of contracts, based on the risk associated with them - avoid situations where you force all your suppliers to deliver the same set of security requirements when it may not be proportionate or justified to do so.

Explain the rationale for these requirements to your suppliers, so they understand what is required from them.

Include your minimum security requirements in the contracts you have with suppliers and in addition, require that your suppliers pass these down to any sub-contractors they might have.

Setting the minimum - four use case studies

Based on your view and understanding of security risk in the context of your supply chain, what minimum security requirements could you set?

Minimum security requirements will vary on a case by case basis. To help clarify how you would go about setting minimum requirements, we present four case studies to illustrate the different approaches that can be taken.

These requirements are not necessarily cumulative, but the measures you can implement to address one use case can be re-used for others. The case studies also present different approaches to assurance that can be used to gain confidence in the management of a range of different risks.

Case A.
Protecting information that you share with suppliers.

You must protect the information you share with your suppliers from any unauthorised access, modification or deletion, which could cause disruption to your organisation and its business.

Example

An IT contractor sold computers stolen from an aviation company which contained details of commercial and military flight plans to pay off debts.

A supplier has a legacy application that wasn't fully patched, yet hosted some sensitive information from the customer.

You should:

- Consider asking suppliers to use Cyber Essentials as the baseline level of protection. It significantly reduces vulnerabilities to the most common internet based threats (hacking and phishing[1]). All suppliers to government are required to demonstrate how they will achieve its five technical controls. Where this level of commitment is not realistic, the new Cyber Security Small Business Guide may provide a more achievable way for suppliers to begin to improve their resilience.
- Where greater assurance is required and you want suppliers to be able to identify with confidence any potential attacker presence on their systems, require suppliers to understand their systems, implement security monitoring and develop an incident response capability.
- To protect against a wider range of attacks, require suppliers to implement a holistic approach to security, following 10 Steps to Cyber Security, ISO27001 (or similar).
- Where appropriate require personnel, physical and procedural controls to protect against fraud, theft, and insider threats. All staff working on a contract should be screened, following the principles outlined by the Cabinet Office Baseline Protective Security Standard (BPSS), and additional checks (eg financial checks) added as required for the role.
- Require the implementation of ICO guidance for protecting and off-shoring personal information, where the personal information is stored, processed or handled as part of a contract.
- Where suppliers use cloud-based services, you should understand that it is not possible to transfer complete responsibility or accountability for protecting information to the provider of that service. This is true in every case. Security requirements to protect information, systems and services should be reflected in the contracts and service agreements you have in place with suppliers, and should inform the choices they make about how the cloud service is deployed and delivered. For HMG, the G-Cloud digital market place, provides a range of service offerings that can be matched against your organisation's needs. As a minimum, it is recommended that suppliers follow NCSC's cloud security principles to frame their security needs.

[1] Note that the NCSC has launched a number of new services under the Active Cyber Defence programme to improve basic cyber security. For example, Mail Check encourages the adoption of secure email protocols for the Public Sector. Anyone can register their DMARC/SPF records and they should. It may be worthwhile recommending these to your key suppliers too.

You must protect the information you share with your suppliers from any unauthorised access, modification or deletion.

Where information is held in a common data environment, whether or not this is cloud-based, it is recommended that this is reviewed using the 'Common Data Environments guidance available on the CPNI website at:

cpni.gov.uk/digital-built-assets-and-environments

Case B.
Specifying security requirements to a supplier who is delivering something to you.

You must ensure that the security properties or requirements needed to protect a product or service, have been effectively specified to the supplier.

Example

A supplier is building a digital service for you that will handle very sensitive information. You have poorly described your security needs and therefore the supplier has delivered something which doesn't deliver the security you need.

You need absolute clarity about your security and functional needs. These must be described clearly and unambiguously to the supplier. If the supplier is delivering an IT system - then it must meet the security requirements that have been specified.

For example, Cyber Essentials or any other needs you have set.

In addition, you should consider:

- Be aware of any known gaps in coverage of schemes like Cyber Essentials.
- Requiring additional controls to provide assurance about the product or service to be delivered. If for example, the contract relates to the development of new software tools, or the manufacturing of components, you will need to specify that the supplier follows best practice in these areas.
- Where a Cloud service is being delivered, you should follow the guidance detailed under Use Case A above.

In cases where a supply chain is delivering a project or asset/facilities management using collaborative digital engineering systems such mitigation methods would not be effective, further guidance is available at:

cpni.gov.uk/digital-built-assets-and-environments

Case C.
Connecting a supplier's systems to yours.

You must ensure that any network connections or data-sharing with third parties does not introduce unmanaged vulnerabilities that have the potential to affect the security of your business systems.

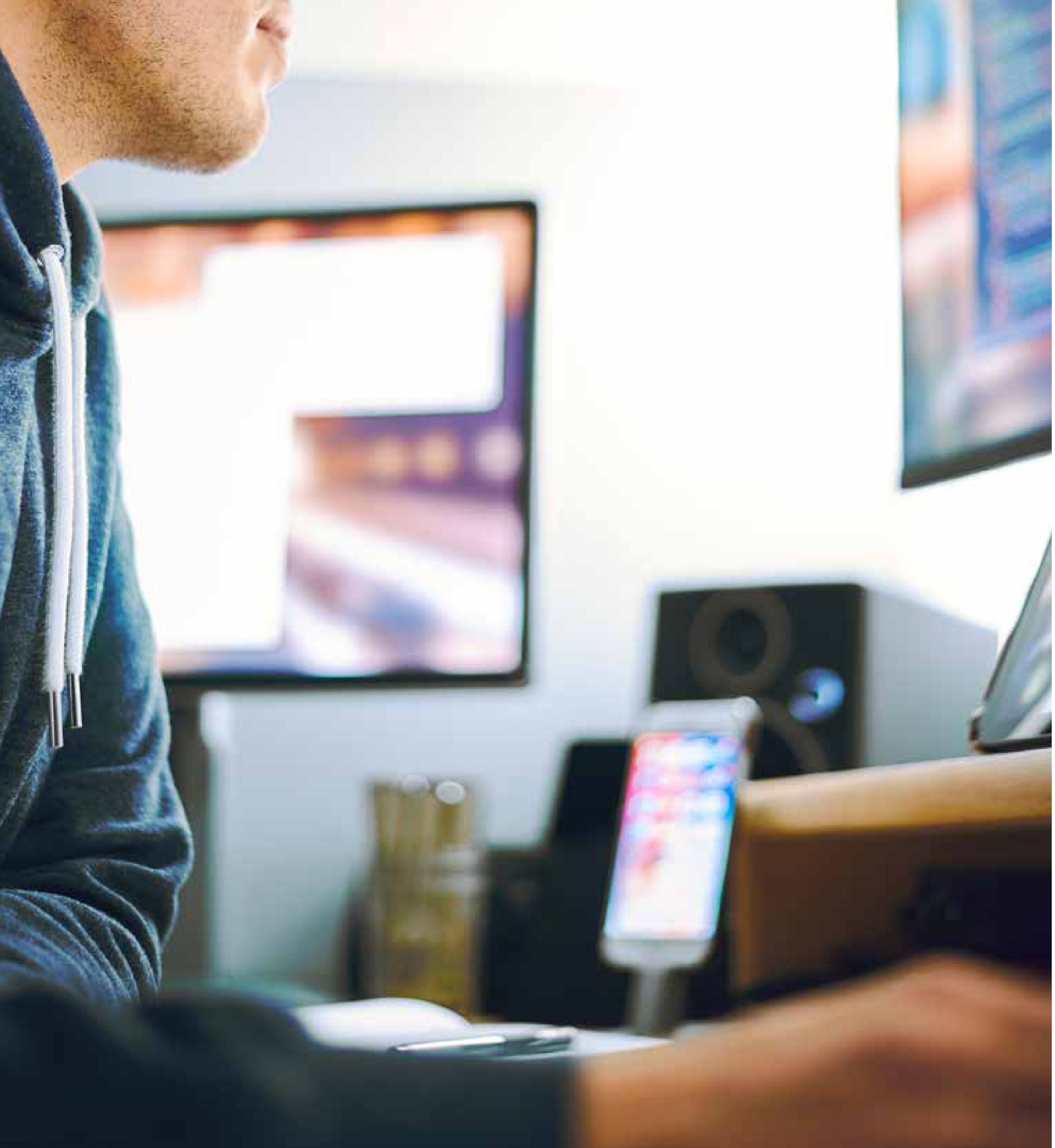
This is a critical consideration for all contracts that include connections to a supplier's system. You will need to decide how you want the supplier to perform the work on your behalf. Will they work at your premises or theirs? How much access and connectivity they will need to carry this out?

Example

Cyber criminals attacked a large commercial company exploiting unprotected supplier connections that were used to manage the customer's environmental control systems. This led to significant loss of data, disruption to business and significant damage to the company's reputation.

Where a supplier's systems are connected to yours you should:

- Ensure that the accesses you provide to your systems, services, information and premises is limited, controlled and monitored. This is true for both your supplier's people and their systems. These accesses should be reviewed periodically, and removed when no longer required.
- Access to contract-related information, contracted products or services should be limited on a 'least privilege' basis.
- If you intend that the supplier will perform the contracted work on your systems and premises, ensure these are appropriately segregated from the rest of your network. 10 Steps to Cyber Security, Network Security shows you how to do this.
- Have a secure means to exchange hard and soft copy information with your supplier. For guidance on hard copy exchanges see the Cabinet Office, Government Classification Scheme and for guidance on data in transit/exchanges see 10 Steps to Cyber Security, Home and Mobile Working and the Walled Gardens Architectural Pattern.
- Where organisations use operational technology as part of a system or to deliver services, like other technology it should be treated as 'untrusted', and managed accordingly.



Case D.
National security case - where a state actor may target you.

You must be confident that your supply chain security can deal with attacks, and attempted subversion by state actors - but only in those circumstances where your threat model warrants it.

Example

A security guard contracted to a defence company stole, and attempted to sell documents that detailed the electronic warfare systems used to protect UK and NATO ships, to a foreign intelligence service.

In national security cases such as this, you will need to seek professional advice from the NCSC and CPNI, as this is beyond the scope of the guidance provided.

Matters will likely include:

- Adoption of bespoke approaches to security.
- Use of high assurance products, with improved personnel and physical security arrangements.
- Vulnerabilities that might arise in manufacturing or build processes.
- Additional measures to protect the privacy and identity of contracting partners and their procurement activities.

6. Build security considerations into your contracting processes and require that your suppliers do the same

Build security considerations into your normal contracting processes. This will help you to manage security throughout the contract, including termination and the transfer of services to another supplier.

Evidence

Require prospective suppliers to provide evidence of their approach to security and their ability to meet the minimum security requirements you have set at different stages of the contract competition.

Providing support

Develop appropriate supporting guidance, tools and processes to enable the effective management of the supply chain by you and your suppliers, at all levels.

You should:

- Ensure the security considerations you build into your contracts are proportionate and align with the various stages of the contracting process.
- Require their adoption in contracts and train all parties on their use.
- Check that your supporting guidance, tools and processes are being used throughout the whole of your supply chain.
- Require contracts to be renewed at appropriate intervals, and require reassessment of associated risks at the same time.
- Seek assurance that your suppliers understand and support your approach to security and only ask them to take action or provide information where it is necessary to support the management of supply chain security risks.
- Ensure that contracts clearly set out specific requirements for the return and deletion of your information and assets by a supplier on termination or transfer of that contract.

7. Meet your own security responsibilities as a supplier and consumer

Ensure that you enforce and meet any requirements on you as a supplier.

Provide upward reporting and pass security requirements down to sub-contractors.

Welcome any audit interventions your customer might make, tell them about any issues you are encountering and work proactively with them to make improvements.

Challenge your customers if guidance covering their security needs is not forthcoming, and seek assurance that they are they happy with the measures you are taking.

Where lessons have been learnt from security incidents, communicate these to all your suppliers, to help them *stop* becoming victims of ‘known and manageable’ attacks.

8. Raise awareness of security within your supply chain

Explain security risks to your suppliers using language they can understand. Encourage them to ensure that key staff (e.g. procurement, security, marketing) are trained on, and understand these risks, as well as their responsibilities to help manage them.

Set goals

Establish supply chain security awareness and education for appropriate staff. NCSC and CPNI awareness materials may be useful.

Information sharing

Promote and adopt the sharing of security information across your supply chain to enable better understanding and anticipation of emerging security attacks. The Cyber Security Information Sharing Partnership (CiSP) is a great example of a free cyber security information sharing service.

9. Provide support for security incidents

Whilst it is reasonable to expect your suppliers to manage security risks in accordance with the contract, you should be prepared to provide support and assistance if necessary where security incidents have the potential to affect your business or the wider supply chain.

Make requirements clear

You should clearly set out requirements for managing and reporting security incidents in the contract.

These should clarify supplier’s responsibilities for advising you about such incidents - reporting timescales, who to report to etc. Suppliers should also be clear about what support they can expect from you if an incident occurs - required ‘clean up’ actions, losses incurred, etc.

GDPR includes fairly short timescales for telling the Information Commissioner about any incidents, so you and your supply chain need to prepare for this.

Propagate lessons learned

Where lessons have been learnt from security incidents, communicate these to all your suppliers, to help them *stop* becoming victims of ‘known and manageable’ attacks.

4 III. Check your arrangements

Businesses will need to gain confidence in their approach to establishing control over their supply chain.

10. Build assurance activities into your supply chain management

- Require those suppliers who are key to the security of your supply chain, via contracts, to provide upward reporting of security performance and to adhere to any risk management policies and processes.
- Build the ‘right to audit’ into all contracts and exercise this. Require your suppliers to do the same for any contracts that they have let that relate to your contract and your organisation. (Note that this might not always be possible or desirable, particularly where this relates to a Cloud service).
- Build, where justified, assurance requirements such as Cyber Essentials Plus, penetration tests, external audit or formal security certifications into your **security requirements.**
- Establish key performance indicators to measure the performance of your supply chain security management practice.
- Review and act on any findings and lessons learned.
- Encourage suppliers to promote **good security behaviours.**

5 IV. Continuous improvement

As your supply chain evolves, you'll need to continue improving and maintaining security.

11. Encourage the continuous improvement of security within your supply chain

- Encourage your suppliers to continue improving their security arrangements, emphasising how this might enable them to compete for and win future contracts with you. This will also help you to grow your supply chain and choice of potential suppliers.
- Advise and support your suppliers as they seek to make these improvements.
- Avoid creating unnecessary barriers to such improvements: acknowledge and be prepared to recognise any existing security practices or certifications they might have that could demonstrate how they meet your **minimum security requirements.**
- Allow time for your suppliers to achieve security improvements, but require them to provide you with timescales and plans that demonstrate how they intend to achieve them.
- Listen to and act on any concerns highlighted through performance monitoring, incidents, or upward reporting from suppliers that may suggest that current approaches are not working as effectively as planned.

12. Build trust with suppliers

- Seek to build strategic partnerships with key suppliers, sharing issues with them, encouraging and valuing their input. Gain their buy-in to your approach to supply chain security, so that it takes account of their needs as well as your own.
- Let them manage sub-contractors for you, but require them to provide you with appropriate reporting to confirm the status of these relationships.
- Maintain continuous and effective communications with your suppliers.
- Look at supply chain management as a shared issue.

6 Example supply chain attacks

A selection of illustrative real-world examples of supply chain attacks.

Outlined below are examples of supply chain attacks that illustrate the challenges organisations face. Attacks are constantly evolving and you should ensure you keep up to date with these. Whilst these are primarily cyber attacks it is important to also consider threats such as fraud, theft and insiders.

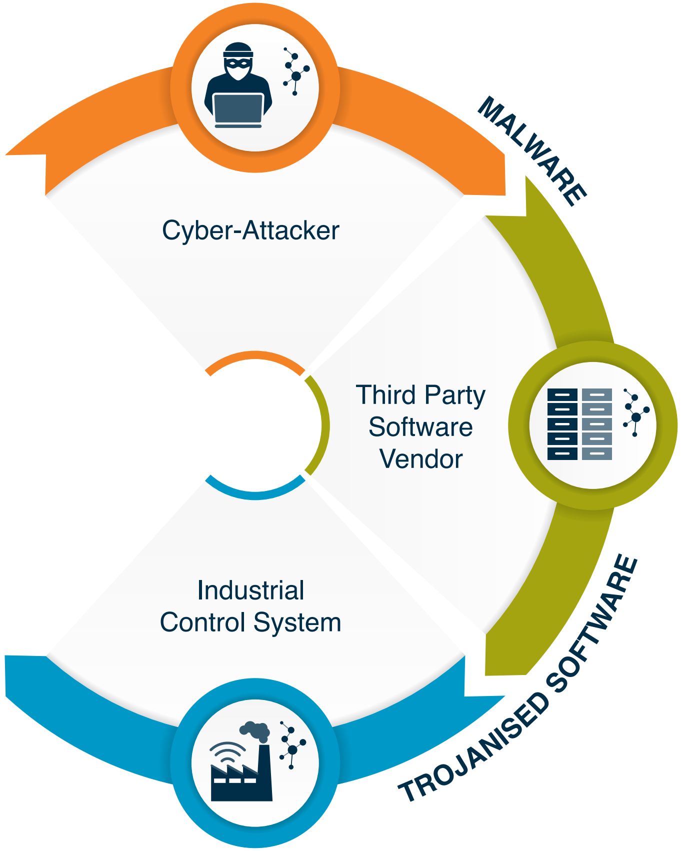
Example 1: Third party software providers

Since 2011, the cyber-espionage group known as Dragonfly (also known as Energetic Bear, Havex, and Crouching Yeti) has allegedly been targeting companies across Europe and North America, mainly in the energy sector. This group has a history of targeting companies through their supply chains.

In their latest campaign, Dragonfly successfuly “trojanised” legitimate industrial control system (ICS) software. To do so, they first compromised the websites of the ICS software suppliers and replaced legitimate files in their repositories with their own malware infected versions.

Subsequently, when the ICS software was downloaded from the suppliers’ websites it would install malware alongside legitimate ICS software. The malware included additional remote access functionalities that could be used to take control of the systems on which it was installed.

Compromised software is very difficult to detect if it has been altered at the source, since there is no reason for the target company to suspect it was not legitimate. This places great reliance on the supplier, as it’s not feasible to inspect every piece of hardware or software in the depth required to discover this type of attack.



Compromised software is very difficult to detect if it has been altered at the source, since there is no reason for the target company to suspect it was not legitimate.

Cyber-criminals also target supply chains as a means of reaching the broadest possible audience with their malware.

Example 2: Website builders

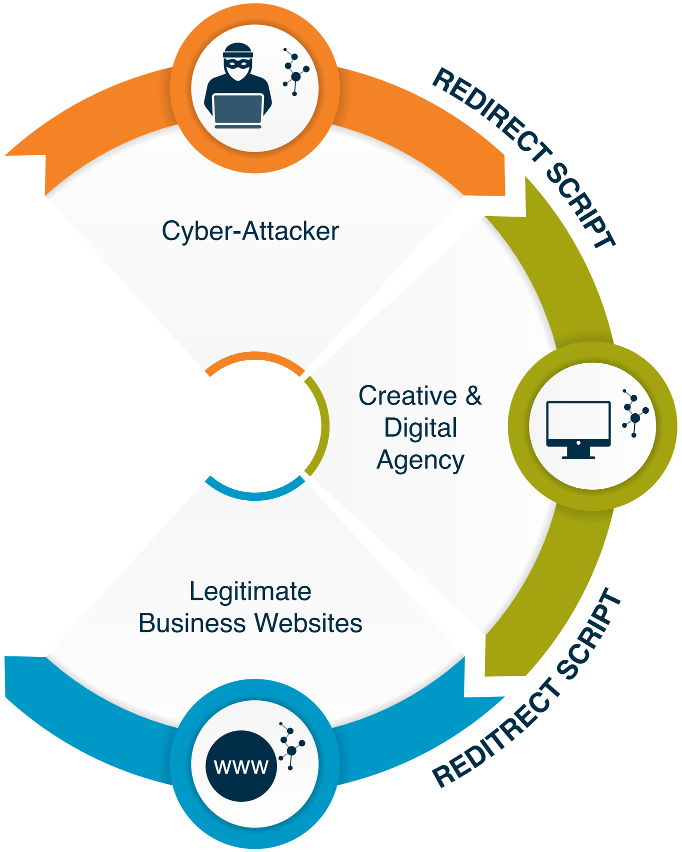
Cyber-criminals also target supply chains as a means of reaching the broadest possible audience with their malware. Identifying and compromising one strategically important element is an efficient use of resources and may result in a significant number of infections.

The Shylock banking trojan is as a good example of this. Focused on e-banking in the UK, Italy and the USA, the threat from the group behind this virus was reduced by a joint operation between law enforcement agencies and the cyber-security community, in July 2014.

The Shylock attackers compromised legitimate websites through website builders used by creative and digital agencies. They employed a redirect script, which sent victims to a malicious domain owned by the Shylock authors. From there, the Shylock malware was downloaded and installed onto the systems of those browsing legitimate websites.

The economy of effort makes this a very successful endeavour. By integrating a multitude of different features adopted from other malware, Shylock was capable of performing customisable 'man-in-the-browser' attacks, avoiding detection and protecting itself from analysis.

Rather than compromising a number of legitimate sites individually, the attack targeted the core script of a website template designed by a UK-based creative, digital agency.



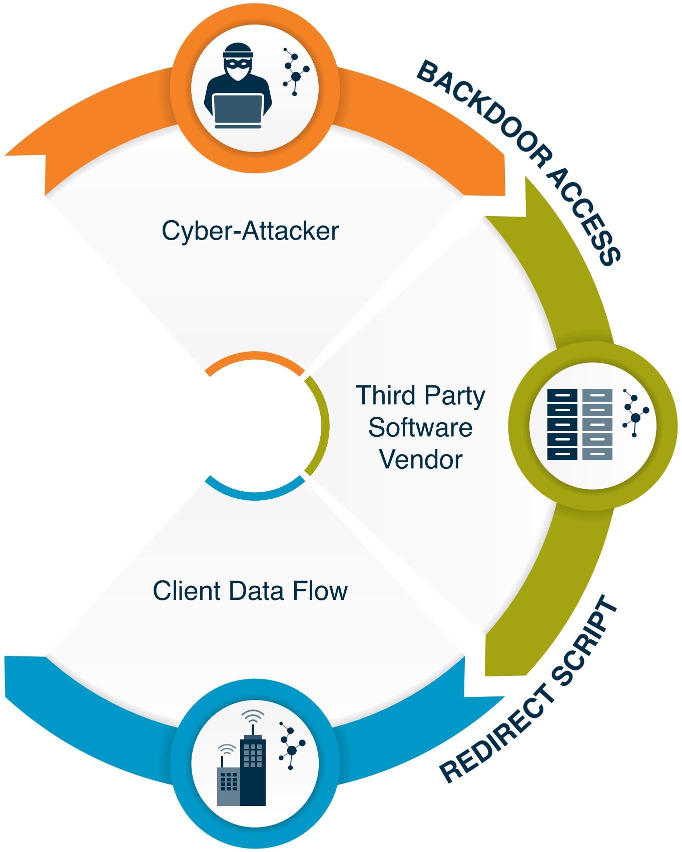
Example 3: Third party data stores

Many modern businesses outsource their data to third party companies which aggregate, store, process, and broker the information, sometimes on behalf of clients in direct competition with one another.

Such sensitive data is not necessarily just about customers, but could also cover business structure, financial health, strategy, and exposure to risk. In the past, firms dealing with high profile mergers and acquisitions have been targeted. In September 2013, a number of networks belonging to large data aggregators were reported as having been compromised.

A small botnet was observed exfiltrating information from the internal systems of numerous data stores, through an encrypted channel, to a botnet controller on the public Internet. The most high profile victim was a data aggregator that licenses information on businesses and corporations for use in credit decisions, business-to-business marketing and supply chain management. While the attackers may have been after consumer and business data, fraud experts suggested that information on consumer and business habits and practices was the most valuable.

The victim was a credit bureau for numerous businesses, providing “knowledge-based authentication” for financial transaction requests. This supply chain compromise enabled attackers to access valuable information stored via a third party and potentially commit large scale fraud.



Such sensitive data is not necessarily just about customers, but could also cover business structure, financial health, strategy, and exposure to risk.

Attackers are increasingly exploiting ‘watering hole’ sites to conduct espionage attacks against a host of targets, across a variety of industries.

Example 4: Watering hole attacks

A watering hole attack works by identifying a website that’s frequented by users within a targeted organisation, or even an entire sector, such as defence, government or healthcare. That website is then compromised to enable the distribution of malware.

The attacker identifies weaknesses in the main target’s cyber-security, then manipulates the watering hole site to deliver malware that will exploit these weaknesses.

The malware may be delivered and installed without the target realising (called a ‘drive by’ attack), but given the trust the target is likely to have in the watering hole site, it can also be a file that a user will consciously download without realising what it really contains. Typically, the malware will be a Remote Access Trojan (RAT), enabling the attacker to gain remote access to the target’s system.

Attackers are increasingly exploiting ‘watering hole’ sites to conduct espionage attacks against a host of targets, across a variety of industries. The VOHO campaign is a good example of this.

References

Pharmaceuticals, Not Energy, May Have Been True Target Of Dragonfly, Energetic Bear

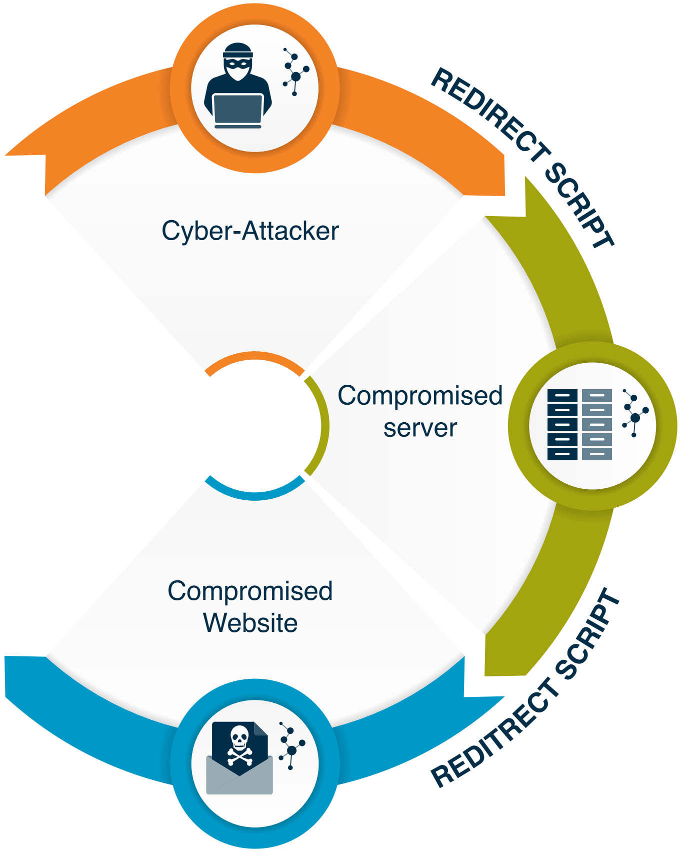
‘Shylock’ malware hit by authorities

Intro to watering holes

Hacking The Street? Fin4 Likely Playing The Market

Data Broker Giants Hacked by ID Theft Service

Espionage Hackers Target ‘Watering Hole’



7 Assessing supply chain security

The table below gives you a series of scenarios against which to measure the security of your supply chain.

The idea is to give you some concrete examples of good and bad supply chain security, to help you begin the process of understanding your own situation.

Good	Bad
You understand the risks suppliers may pose to you, your wider supply chain and the products and services you offers. Know the sensitivity of information your suppliers hold and value of projects they are supporting.	You have a poor understanding of the risks that suppliers may pose to you, your wider supply chain and the products and services it offers. You do not know what data they hold, nor the value of projects they are supporting.
Know the full extent of your supply chain, including sub-contractors.	Only know your immediate suppliers, but have limited/no knowledge of any sub-contractors.
Know the security arrangements of your suppliers and routinely engage with them to confirm they are continuing to manage risks to your contract effectively.	Have no real idea about the security status of your supply chain, but think they might be okay. Fail to review this status.
Exercise control over your supply chain, exercise your right to audit and/or require upward reporting by your suppliers to provide security assurance that all is working well. An audit request would not be your first interaction with the supplier.	Exercise weak control over your supply chain, lose sight of sub-contracting, fail to exercise audit rights, do not seek upward reporting. Often, the first engagement of your security team with the supplier will be for an audit following an incident.
Based on your assessment of risks and the protections you deem are necessary, set minimum security requirements for suppliers, telling them what is expected in contracts.	Fail to set minimum security requirements, leaving it up to suppliers to do their own thing, even though they might not have the security awareness to understand what is needed, or know how to do this effectively. Or set minimum security requirements, but fail to match these to your assessment of the risk - potentially making security unachievable for many of your suppliers.
Differentiate the levels of protection required to match the assessed risks to the specific contract. Ensuring these protections are justified, proportionate and achievable.	Set a disproportionate 'one size fits all' approach for all suppliers, regardless of the contract and assessed risks. Fail to ensure these controls are justified and achievable - potentially causing suppliers not to compete for contracts with you.
Require that the protections you have deemed necessary in each case are passed down throughout your supply chain. Check to ensure it is happening.	Leave security to immediate suppliers to manage, but fail to mandate and/or check it is happening.
Meet your own responsibilities as a supplier (and challenge your customers for guidance where it is lacking). Pass your customer's requirements down and provide upward reporting.	Neglect your responsibilities as a supplier, or ignore any absence of customer guidance. Fail to pass requirements down, and/or fail to provide upward reporting.
Provide some guidance and support to suppliers responding to incidents. Communicate lessons learned so others in your supply chain avoid 'known problems'.	Offer no incident support to your suppliers,. Fail to act or spot where 'known issues' might impact others in your supply chain, nor to warn others about these issues - potentially leading to greater disruption: with known issues hitting many suppliers.

Good	Bad
Promote improvements to the cyber awareness of your suppliers. Actively share best practice to raise standards. Encourage suppliers to subscribe to the free CISP threat intelligence service so they can better understand potential threats.	Expect suppliers to anticipate developing cyber attacks offering little or no support or advice, regardless of their security awareness and capabilities.
Build assurance measures into your minimum security requirements (such as Cyber Essentials Plus, audits and penetration tests). These provide an independent view of the effectiveness of your suppliers security.	Fail to include assurance measures into your security requirements, trusting that your suppliers will do the right thing - regardless of whether they have enough knowledge or experience to know what is expected of them.
Monitor the effectiveness of the security measures that are in place. Based on lessons learned from incidents, feedback from assurance activities, or from suppliers about issues, be prepared to revise or remove controls that are proving ineffective.	Fail to monitor the effectiveness of security measures. Fail to listen to feedback. Be unwilling to make changes, even when the evidence in favour of doing so is overwhelming.

8 Assessing supply chain management practice

It is expected that your will already be following good procurement and contracting practice.

This guidance offers additional factors that you may consider.

Good	Bad
Develop partnerships with your suppliers. If your suppliers adopt your approach to supply chain security as their own, there's much greater potential for success than if you simply mandate compliance.	Dictate requirements without consultation.
Get suppliers thinking about security from the outset by starting the discussion about security earlier than you would during traditional product assurance engagements.	Just consider security to be a product assurance issue.
Explain benefits of achieving the required security improvements to suppliers: i.e. that these will meet compliance requirements, or offer the potential for the supplier to win other contracts.	Just tell your suppliers what to do, but offer no explanation of benefits: some suppliers may consequently be reluctant to bid for contracts.
Consider how you will enable suppliers who may require legitimate but ad hoc/ occasional and/or limited access to your business to do so without having to comply with your minimum security requirements for suppliers. Document the procedures for these engagements and train all parties on their use.	Make no provisions for such circumstances,and either require them to meet your security requirements (even though their is little justification for this), or ignore it and let people make their own arrangements (hoping it will be okay).
Where required, develop common contract artefacts (i.e. risk assessment and self-assessment security questionnaire) to support the contracting process and to enable your suppliers to pass these down to sub-contractors. Share these with your suppliers and train all staff on their use.	Offer little/no advice on the contracting process, allowing suppliers to do their own thing - and fail to understand the implications of this in terms of assurances about overall supply chain security.
Require these artefacts to be reviewed at appropriate intervals, such as at contract renewal, when there are significant changes, or in response to major incidents.	Worry about the initial contract, but take little/no interest in subsequent contract renewals: fail to spot changes/problems that may have arisen.
Ensure that security considerations are an integral part of the contract competition process and that it influences the choice of supplier.	Only worry about security at the end of the contracting process - these considerations have little influence on your choice of supplier.
Require suppliers to provide appropriate evidence of their security status and ability to meet your minimum security requirements throughout the various stages of the contract competition: perhaps seeking basic assurances of your supplier's ability to meet legal and regulatory requirements, as a first gate, at initial contract advertisement, but requiring greater detail as the competition narrows to a choice of a few preferred bidders.	Ask for more information than you need, can handle, or will use: potentially creating unnecessary workloads on potential suppliers when they have little chance of winning the contract. Be surprised when suppliers do not compete for contracts on these grounds.

Good	Bad
Ensure these do not impose unnecessary workloads on prospective suppliers - particularly in the early stages of contracting when there are many applicants for the contract.	Just dust off an existing ISO27001 based questionnaire that you think might do and get suppliers to complete that: even if this has no resemblance to the minimum security controls you have used (i.e. Cyber Essentials or 10 Steps to Cyber Security).
When using a self-assessment security questionnaire to aid the contracting process, ensure this matches the minimum security requirements you have set - and reduces workloads on suppliers to a necessary minimum. Only requires more detailed information when the supplier has progressed to the later contracting stages and is one of a very small number being considered for the contract.	Fail to take account of the workloads this will create for suppliers, nor seek to match your requirements to the stage of the contract competition.
Allow suppliers time to achieve desired security improvements: develop risk criteria to manage this transition (i.e. require suppliers to provide a security improvement plan setting out how progress will be made) and stipulate when checks against progress have been made and should be performed.	Set unrealistic deadlines, or have no clear or consistent risk criteria to inform decisions about suppliers who are unable to make these improvements within agreed time frames. This may mean you are unable to work with such suppliers – potentially leading to a damaging fall in capability and reduced choice of suppliers.
Acknowledge any existing security certifications or prior/existing contract approvals that suppliers may have, and allow them to re-use such evidence to demonstrate how this might meet some of your minimum security requirements. But probe appropriately to confirm this is the case.	Ignore any existing security certifications, or contract approvals, requiring suppliers to achieve compliance with your minimum security requirements regardless. This could create unnecessary work and cost for suppliers, harming these relationships.
Expect all suppliers to achieve Cyber Essentials. But understand that some suppliers - even those who have existing security certifications like ISO27001, may find it difficult to meet the letter of the scheme. However, where the letter of the scheme cannot be met for whatever reason, you should seek to understand what steps the supplier is taking to manage these risks through for example alternative business processes or compensating security controls. You should check to confirm these are suitable.	Expect all suppliers to achieve Cyber Essentials, but adopt a black and white approach taking no account of special circumstances. Do not acknowledge any difficulties and refuse to award contracts to suppliers who find Cyber Essentials certification difficult to achieve, further undermining your own capability and choice of suppliers.
Provide some mapping of the minimum security requirements you have chosen to common commercial security schemes to help suppliers re-use evidence, and other customers to assess equivalences. This will also help suppliers demonstrate how they align with international schemes.	Provides no support, expect suppliers to do this mapping themselves: potentially increasing workloads and leading to inconsistencies - potentially undermining customers trust in the evidence they provide.
Monitor and continually improve the process, discontinuing or refining processes that are disproportionate, ineffective or unjustified.	Allow disproportionate, ineffective or unjustified processes to remain unchanged. Fail to listen to consistent, justified calls for refinement.

9 Supply chain security: 12 principles

Principals of supply chain security

How to gain and maintain control of your supply chain

The principals are divided into four stages representing the process of securing your supply chain.

To find out more visit: www.ncss.gov.uk/guidance/supply-chain-security

i. Understand the risks

- Understand what needs to be protected and why
- Know who your suppliers are and build an understanding of what their security looks like
- Understand the security risk posed by your supply chain

ii. Establish control

- Communicate your view of security needs to your suppliers
- Set and communicate minimum security requirements for your suppliers
- Build security considerations into your contracting processes and require that your suppliers do the same
- Meet your own security responsibilities as a supplier and consumer
- Raise awareness of security within your supply chain
- Provide support for security incidents

iii. Check your arrangements

- Build assurance activities into your approach to managing your supply chain

iv. Continuous improvement

- Encourage the continuous improvement of security within your supply chain
- Build trust with suppliers

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 favour 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 judgment as regards use of this document and seek independent professional advice on your particular circumstances.