UK SPACE AGENCY

Cyber Security Toolkit

CYBER SECURITY TOOLKIT - SPACE ASSETS

1. INTRODUCTION

i. Space applications are embedded right across our society. They underpin a wide range of core daily activities that almost everyone now takes for granted, and are critical to supporting the military, security, intelligence, emergency, disaster management and resilience services.

ii. There is a present and increasingly significant threat to vulnerable space assets; their strategic nature makes them a specific target for a wide range of cyber-attacks that could manipulate or disrupt essential services and potentially destroy or weaponise them, demonstrating a clear requirement for an enhanced and robust cyber security regime.

iii. It is recognised that the space sector has grown at speed, being encouraged to develop at pace in response to the market; the pace of change has meant that robust security structures and resilience measures have often lagged behind. Unless we address this issue the UK carries the risk of losing substantial ground in the sector, falling behind its competitors as vulnerabilities are exposed and presenting a substantial risk to our national interests and critical infrastructure that relies on the services the sector provides.

2. SCOPE

i. This toolkit is aimed at those who supply services or develop, build and own assets within and for the space sector.

ii. For the purpose of this document, assets are facilities, systems, networks or processes and the essential workers that operate and facilitate them. The loss or compromise of these could result in major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity if compromised, could result in significant economic or social impacts for customers and/or the UK as a whole.

iii. This document details the scoping that asset owners should undertake to establish their dependencies and therefore vulnerabilities, assess risk and based on these results, adopt an appropriate cyber security strategy.

iv. This toolkit does not detail physical and personnel security requirements or specific technical measures in order to mitigate risks. The National Cyber Security Centre (NCSC) https://www.ncsc.gov.uk/ and the Centre for the Protection of National Infrastructure (CPNI) https://www.cpni.gov.uk/physical-security can provide assistance and advice in these matters.

3. FORMS AND TECHNIQUES OF CYBER ATTACKS

i. There are a number of forms of cyber-attack. A common feature is that the technical aspects of individual attacks frequently mutate on a daily basis. Attacks include (but are not limited to) social engineering, access compromise and supply chain corruption.
Some of the most commonly used techniques are outlined in the table below.

ii. Social engineering

Social engineering is the manipulation of individuals to carry out specific actions, or to divulge information. The information gained is frequently used as an enabler of cyber-attacks.

Operations security is particularly susceptible to social engineering tools and techniques as these exploit knowledge at the personal level, meaning attackers can become aware of activities, intentions, capabilities and vulnerabilities.

Social engineering is commonly used to enable the delivery of malicious software onto target systems. In many cases the threat actor using these methods will have carried out extensive research on the target to maximise their chances of success.

iii. Access compromise

Access is crucial to the success of any cyber-attack and can be obtained in three ways: physical, close and remote.

- Physical access is the ability to gain direct access to a computer or network, such as by connecting a USB device directly to a computer.
- Close access is the ability to access to a computer or network from deployed platforms, people and equipment operating within the area of that network but do not have physical access. Typically this could be through use of the electromagnetic spectrum, such as connecting via Wi-Fi. Alternatively, close access can be achieved by an adversary installing specific types of malicious software on a device.
- Remote access is the ability to get access to a computer or a network from external locations (physical and virtual) that may be considered outside of that network.

iv. Supply chain corruption

Unscrupulous and/or malicious suppliers may interfere with the supply chain resulting in untrusted or unaccredited equipment being delivered, which may not function properly, safely, and/or securely. Such interference can result in malware or maliciously modified components being embedded in newly delivered or recently repaired electronic equipment.

It is recognised that assuring every part of the supply-chain is a difficult and laborious process however every effort should be made to ensure all components including hardware and software has a clear line of supply, should be from trusted suppliers where possible and can be traced back to the supplier and country of origin.

Types of cyber-attack

	Form of attack	Technique
A	Installation or execution of unauthorised/malicious software	These can contain malicious software, viruses, spyware and ransomware which can crash IT systems or provide unauthorised access to confidential and/or business data.
B	Physical loss, theft or damage of an IT asset	Includes all data storage including removable media.
C	User impersonation	Includes password sharing, attacks on authentication controls, zombie user accounts etc
D	Suspicious privilege amendment	Instances where a genuine user appears to have been placed in an inappropriate user group or have gained excessive privileges
E	Suspicious use of legitimate privileges	Where a user appears to have abused existing privileges such as accessing large numbers of files/records, copying data to removable media devices or emails etc
F	Eavesdropping on a communication channel	Suspected, attempted or actual instances where data appears to have been intercepted by an unauthorised party. Includes instances where sensitive data is transferred to authorised recipients in unencrypted form.
G	Service Spoofing	Suspected, attempted or actual instances where a data service is spoofed by a third party.
H	Service Jamming	Use of overwhelming electronic transmissions to overwhelm legitimate signals
I	Denial of Service	Suspected, attempted or actual instances where an entity places an excessively high demand on a system or asset.
J	Phishing	Suspected, attempted or actual instances where persons receive an email which claims to be something, or from someone, that it is not.

The primary threats to space assets and activities could come from any of the following which can be defined as "hostile actors":

Foreign States	States that wish to cause damage or harm to the UK or advance own national capabilities by shortcutting development timeframes; through various means, such as cyber-attacks or espionage
Terrorists	Groups that may seek to cause harm to the economy as a whole, or carry out attacks to advance political agendas or in attacks designed to result in mass casualties
Criminal organisations	Any organisation seeking to acquire information, goods or other through illegal activity
Hacktivist groups	A person or group who gains unauthorised access to computer files or networks in order to further social or political ends
Individual hacker	A person who gains unauthorised access to computer files or networks in order to gain personal satisfaction
Insider threat	The potential for an individual who has or had authorized access to an organsation's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organisation

There is a high level of mobility between the threat groups (ie criminal organisations acting as proxies for foreign states, individual hackers providing resource to criminal organisations to carry out a specific mission and so on).

Common across all threats is the difficulty of attribution of the source of an attack. The highest levels of certainty can only be achieved after detailed forensic and circumstantial investigations.

4. RECOMMENDED ACTIONS

It is recommended that space asset owners and suppliers of goods to the industry undertake the following activities in order to determine the level of defense their assets and activities require:

i. Anticipate weaknesses - dependency/vulnerability mapping

It is necessary to identify the operation of essential functions, critical physical assets, along with critical personnel roles, that could be comprised.

All hardware, software, third party services, and dependencies on supply chains that support the complete life cycle of the asset should be included in the mapping to establish where vulnerabilities may lie.

Your results of the mapping questionnaire at Section one will inform the level of risk currently in place and the impacts of loss, temporary or otherwise, of your supplies or asset.

ii. Calculate the risk - Impact assessment

The likelihood of a cyber-attack against space assets has increased over recent years, representative of increased hostile state activity, easier access to tools and more developed skills. Although all cyber-attacks have the ability to cause significant damage, should an adversary gain access to control systems within the sector this could generate devastating impacts. A potential attacker does not require physical access to conduct disruptive or destructive attacks.

The impacts caused from malicious cyber activity may not be immediately detected or fully realised until significant damage has been done or for some time after the attack itself.

Reputational impacts may be considerable and confidence may be lost due to the perception that the victim was unable to adequately protect their systems, or they considered investment in security unnecessary.

Cyber risks are contained within a constantly evolving threat landscape as new tools and skills are developed and become easier to acquire. Dynamic risk assessments on a continuous rolling basis are vital to keep pace with these abilities and new technology used both by the perpetrators and space asset developers and owners.

Risks should also not be treated in isolation but should be combined with a more systemic analysis which includes physical and personnel related risk vectors.

Without a regular systematic programme of risk assessment many systems remain vulnerable to attack, because the mitigating actions are not aligned with the changing risks.

Cyber security is not just an I.T. issue and should be embedded within the culture of the business with oversight at the highest level within the company.

Following an assessment of dependencies/vulnerabilities as in Section one, asset owners and suppliers of goods to the space industry can move on to assessing their level of impact risk.

An impact assessment table can be found at Section two. This should be used to assess the impact of loss of each asset, determine the worst case scenario, and ultimately define the mitigation measures suitable as detailed at Section three. The higher the level of risk, the more comprehensive the cyber-security measures should be, leading to greater depth of protection and awareness. In contrast, if the risk is lower, then security may be provided for with less extensive measures, provided a minimum standard is met.

iii. Mitigate the risks – Adoption of a cyber security system

All asset owners should draw up and maintain a cyber security strategy relating to its information systems and space activities. Strategies should follow best practice guidance and advice from the NCSC.

Space asset cyber-security should be appropriate and proportionate based on the level of risk and assessment of impact of loss as determined by the asset owner using the table in Section two.

Where there are no existing license requirements or regulation in place for the activity being undertaken the recommended level of cyber security adoption is at Section three below.

iv. Reporting

Disclosure of cyber-attacks so everyone can learn and assist in remediation and develop an intimate knowledge of the threat with transparency shows that an organisation is diligently managing the risks.
Section four covers reporting requirements both legally and voluntarily.

v. Business Continuity, organisational recovery and response

Considering how to continue your ability to carry on your space related activities in the event of a cyber-attack is essential.

Having a Business Continuity Plan (BCP) enhances an organisation's ability to notify and triage incidents sooner and more importantly be dealt with expeditiously at the appropriate level, and consequently manages the impacts that the cyber incident will have.

Section five is a starting point to ensure that Business Continuity Plans include organisational impacts due to cyber-attack, in order to minimise disruption, prepare and document alternative options for supply chains and assets.

SECTION ONE

SECTION ONE - DEPENDENCY/VULNERABILITY MAPPING

All involved in the supply chain, production and ownership of space assets should consider the following questions in order to identify their vulnerabilities and dependencies.
The responses to these questions should be documented as an evidence base of risk and regularly reviewed as asset use and technology changes.

A. What cyber security is already in place?

B. Testing and exercising:
i. What cyber scenario based exercising have you undertaken to examine the most likely and worst case impact scenarios?
ii. What cyber-attack penetration testing has been performed on either the ground operations/control or spacecraft/satellite infrastructure?

C. What specialist staff training in cyber security protection and response is in place?

D. What assets, parts and/or services do you have that could be affected by a cyber-attack?
For each of these:
i What is the possible extent of the disruption? (what services are impacted, what is the result of this);
ii What would the likely cost of any disruption/loss? (replacement of asset/parts)
iii What is the potential length of time of any disruption? (length of time for a fix, replacement of parts)

E. Which services and/or parts are critical to the working of the asset?

F. Do you intend to perform remote access to any part of the space asset?
And, if so,
i. What controls are in place to secure desktop logins?
ii. What measures are in place to confirm the identity of users?
iii. What controls are in place to restrict access should users not be able to be authenticated?
iv.What procedures are in place to recover legitimate access if accounts are locked out?

G. Supply Chain;
There needs to be a clear and documented route of supply for all parts, supplies.
This should include;

- Country of origin
- Assurance processes in place either by the supplier/manufacturer or yourself
- What alternative sources of supply are there, if any? (Are you aware whether there are available substitute parts available on the market and the lag time for manufacture/delivery. Are there multiple suppliers should there be more than one supply chain loss?)

(For each of these assets, parts and/or services part of your supply chain re-ask yourself the questions at A - C. in this section).

The second way in which you are likely to be impacted through poor cyber security of your supply chain is through them being used as a backdoor to gain access to your network.

i. Do any suppliers have access to your network?

- Detail who these are and the accesses they have.
- Consider whether access is really needed.
- Consider whether the scope of their access is appropriate (do they have access to areas/services they have no need for)
- What processes are in place to confirm the identity of those accessing your systems?
- What cyber security processes/assurance do these suppliers have? (All should undertake the assessments as covered in this document)

ii. What processes are in place to ensure only the necessary access is made available to suppliers and other access is secured?

Detailed guidance on supply chain security can be found on the NCSC site at:
https://www.ncsc.gov.uk/collection/supply-chain-security

SECTION TWO

SECTION TWO - IMPACT ASSESSMENT MATRIX

	REPUTATIONAL DAMAGE	COST	RECOVERY TIMESCALE
	The impact that the loss/compromise of the asset has on reputation for all those within the R&D, build, launch, ownership and sponsorship chain. This includes all educational establishments involved, suppliers of parts, key partners and UK PLC.	*The direct cost of damage and cost of economic output lost (business interruption) as a result of the loss/compromise of the asset. This includes the cost of any damage to the asset itself.*	*The ability to recovery the asset to its original or enhanced ability. Delays in recovery due to rebuild time or difficulty obtaining parts required from original or alternative suppliers.*
CATEGORY 5 (Catastrophic)	Catastrophic loss of business, damage to international relationships and professional reputation within the sector equating to closure of the business/insolvency.	Cost of recovery/replacement of asset not viable with company finances. Directors' personal assets pursued through the courts.	Catastrophic damage long term (more than 1 year) or complete loss of asset indefinitely.
CATEGORY 4 (Significant)	Significant loss of business. Loss of confidence by shareholders leading to voting action against multiple members of the Board. New clients refuse to engage or contracts with existing customers not renewed or terminated. Significant media attention.	Company value impacted. Vulnerability to hostile mergers & acquisitions actions increased or achieved. Public liability and other insurances declined/withdrawn or subject to special conditions. Company restructured. Loss of workforce. Costs (cash and opportunity) incurred through defending legal action.	Significant damage to the asset resulting in up to 1 year to resumption of normal commercial operations.
CATEGORY 3 (Moderate)	Moderate loss of business and professional reputation. Customer(s) lost. New customers needed to restore financial stability. Reports in specialist media. Disclosure report to regulators. Business practices reviewed and amended.	Liquidated damages pursued by client. Financial losses cannot be contained internally. External finance required to raise necessary capital for event remediation. Staff laid off or contractors' engagements terminated. Public liability insurance premiums rise. Directors' dividends impacted.	Moderate damage to the asset resulting in up to 6 months to resumption of normal commercial operations.

CATEGORY 2 (Minor)	Minor loss of business. Disclosure required to customer. External stakeholder reassurance campaign required.	Disclosure required to insurance companies. Interruption to company cashflow. Cost of recovery covered by reallocation of cash from other projects across the business.	Minor damage to the asset resulting in up to 3 months to resumption of normal commercial operations.
CATEGORY 1 (Limited)	Event contained within the company.	Cost of recovery contained within normal project contingency provision.	Limited damage to the asset. Up to 1 month to resumption of normal commercial operations.

Based on the recognised national criticality scales with tailoring specific to the space sector.

Hitting any one of the above categories equals the overall risk to the asset, for example an asset may be considered to have a minor impact on customers but require significant costs to recover the asset to full working order, therefore the overall risk would be ***significant.***

SECTION THREE

SECTION THREE - MITIGATION: ADOPTING A CYBER SECURITY REGIME

There should be a systematic process in place to ensure that identified risks are managed and there is confidence that mitigations are working effectively. Confidence can be gained through, for example; product assurance, monitoring, vulnerability testing, auditing and supply chain security.

The NCSC assurance guidance provides some examples that may be useful to understand cyber security confidence in your organisation and there are some specific technical NCSC guides covering Penetration Testing and Cloud Security.

All suppliers and owners of space assets as a baseline should look to achieve a Cyber Essentials Plus certification.
This is an independently assessed entry level assessment which allows you to have a clear picture of your current cyber security and a recommendation of security controls which should be put in place.
Further details can be found at https://www.cyberessentials.ncsc.gov.uk/

Additionally, depending on the risk level assessed in the previous section, suppliers and owners of space assets should seek to achieve the following cyber security standards as laid out in the table below.

RISK LEVEL	Essential standard/s	Additional considerations
5 (Catastrophic)	ISO 27001, ISO 27002 & ISO 27035-1	At least 1 security professional working in the relevant field should aim to acquire certification as a SCADA Security Architect (CSSA) ISO 28000:2007
4 (Significant)	ISO 27001 & ISO 27002	ISO 27035-1 & ISO 28000:2007
3 (Moderate)	Cyber Assessment Framework (CAF)	ISO 27001
2 (Minor)	Cyber Assessment Framework (CAF)	
1 (Limited)	Cyber Essentials Plus only	

Further information regarding each of the recommended standards is detailed below.

The Cyber Assessment Framework (CAF) and CAF Guidance

While it is not possible to devise an effective set of prescriptive rules for good cyber security, it is possible to state a set of principles as a guide to cyber security decision-making. The NCSC has developed such a set of principles as part of the CAF.

The CAF cyber security principles define a set of top-level outcomes that, collectively, describes good cyber security for organisations performing essential functions. Each principle is accompanied by a narrative which provides more detail, including why the principle is important. Additionally, each principle is supported by a collection of relevant guidance which both highlights some of the relevant factors that an organisation will usually need to take into account when deciding how to achieve the outcome, and recommends some ways to tackle common cyber security challenges.
https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance

ISO 27001

A management system that is intended to bring information security under management control and gives specific requirements. Covering:

- A systematic examination of the organisation's information security risks, taking account of the threats, vulnerabilities, and impacts;
- Design and implementation of a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adoption of an overarching management process to ensure that the information security controls continue to meet the organsation's information security needs on an ongoing basis.

ISO 27002

This provides best practice recommendations on information security controls for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). Covered is:

- Physical and environmental security
- Human resource security
- Access control

Certified SCADA Security Architect (CSSA)

CSSA is a professional certification from the Information Assurance Certification Review Board, a non-profit organisation formed by information security professionals.
CSSA contains the following domains:

- SCADA security policy development
- SCADA security standards and best practices
- Access Control
- SCADA protocol security issues
- Securing field communications
- User authentication and authorization
- Detecting cyber-attacks on SCADA systems
- Vulnerability assessment

ISO 27035-1

This outlines the concepts and principles underpinning information security incident. It describes an information security incident management process consisting of five phases, and says how to improve incident management.
The standard lays out a process with 5 key stages:

- Prepare to deal with incidents e.g. prepare an incident management policy
- Identify and report information security incidents;
- Assess incidents and make decisions about how they are to be addressed
- Respond to incidents i.e. contain them, investigate them and resolve them;
- Learn the lessons

ISO 28000:2007

This is specification for security management systems for the supply chain.
It looks at the requirements of a security management system particularly dealing with security assurance in the supply chain.

SECTION FOUR

SECTION FOUR - REPORTING

Timely incident reporting is important especially where an assailant is using techniques already known to experts such as the National Cyber Security Centre (NCSC). Defences or remediation approaches may already have been determined which can aid your organisation by significantly shortening the remediation activity.

Incident reporting should be made to the following appropriate organisations:

Information Commissioners Office

The General Data Protection Regulation (GDPR) came into force on 25 May 2018 and places robust safeguards over the handling of personal data.
Any organisation that suffers a cyber incident involving breach of personal data, or any Operator of Essential Services which experiences disruption of service due to a cyber-attack, may be legally mandated to report to the Information Commissioner's Office (ICO) (under General Data Protection Regulations (GDPR)) or their Competent Authority (CA) (under The Security of Network & Information Systems Regulations – NIS Regulations) respectively. There are strict timings for reporting to the ICO which differ depending on the type of incident. Details can be found at https://ico.org.uk/for-organisations/report-a-breach/

Action Fraud

Fraud and cybercrime should be reported to Action Fraud at www.actionfraud.police.uk. Organisations which are currently suffering a live cyber-attack (in progress), should call 0300 123 2040 immediately. Specialist advisors are available 24 hours a day, 7 days a week.

NCSC

Significant incidents[i] should be reported to NCSC via www.ncsc.gov.uk/report-an-incident (monitored 24/7). NCSC will triage the incident type to determine the level of national response required, if any and will liaise with reporting companies as necessary.
NCSC will not share information without permission.

UK Space Agency

The importance of sharing cyber activity knowledge amongst those who need to know should not be underestimated.
Incidents involving space based assets and systems should be reported to resilience@ukspaceagency.gov.uk providing as much information as possible in order for assessment to be made whether the attack is likely to spread or have severe impacts on the UK population, economy and/or critical services.

The UKSA may share knowledge of the attack with others in the space community (anonymising the affected organisation's information) in order for others to undertake mitigation measures.

Depending on the scale of the incident information may also be shared with machinery of government processes in order for the wider impact on the UK to be assessed and managed.

Reports should contain as a minimum:

1. Organisation
2. Contact name, role in the org, tel, email

3. Date and time of attack (if known)
4. Type of attack
5. Asset affected and normal role of that asset
6. Impact/s
7. Timescale for remediation

Reporting to NCSC is encouraged for all incidents and you may be required to report to other Government Departments and Agencies under licensing and legislative requirements depending on the role undertaken by the asset or your organisation.

The UKSA and NCSC will gather data for trend analysis and improve our education and awareness of the space sector community and the issues arising. This anonymised information will be shared with the Space community.

[i] A 'significant' incident is one which poses a serious risk to the ongoing operation or to its customers. This could include attacks which disrupt the provision of essential services to the public, or which result in a significant loss of key data such as sensitive information or intellectual property.

SECTION FIVE

SECTION FIVE – RECOVERY

Cyber-attacks continue to evolve with some becoming increasingly indiscriminate, so unfortunately it is almost inevitable all organisations are at risk sooner or later.

Designing a plan stating how you will respond in the event of a cyber-attack on space assets will pay huge dividends in clarifying a number of key things, which will also support and inform both Business Continuity requirements and recovery priorities.

Business Continuity Measures (BCM) and recovery planning is a continuous process to help your organisation anticipate, prepare for, respond to and recover from disruptions. Plans should be considered for all incidents which may affect normal business including a cyber-attack against any system, however for the purpose of this guidance only space assets are being considered.

When assessing the recovery from a cyber-attack it is crucial to firstly consider:

1. What is the acceptable level of service agreed for each space asset? (Some activities may need to be scaled up whilst other noncritical activities might be able to be scaled down or suspended).

2. Does the loss of the space asset impact elsewhere in your organisation, others who are dependent upon your service or on those in the supply chain, creating risks that could threaten the performance of wider and/or critical functions?

Documentary evidence that a systematic approach to considering all space-based supplies and assets is essential to ensure there are no gaps in thinking.
Using the information gathered in the mapping exercise in *Section one* of this guidance; Business Continuity and recovery plans should detail:

1. How the response to the cyber-attack will be managed, and thereby limit the impact this could have on ongoing operations
2. Alternative suppliers of goods/assets, timescale for production and delivery
3. Details of your or any other redundant back-up systems which are an adequate replacement (include details stating how to initiate this, length of time these would take to put into action, cost, etc.)
4. Ownership for key tasks and contact details for decision makers
5. A communications strategy including escalation to the UK Space Agency where any asset is damaged or lost and there is an impact on the UK public and/or government services

Training an appropriate number of suitable staff is vital and should include the contents of the plan, roles and responsibilities and the skills and knowledge required.

Plans should be tested and exercised with those with a responsibility to act on the plan on a regular basis to ensure that they are effective. The frequency of these exercises will depend on the rate of change and the outcomes of previous exercises. If weaknesses are identified, your plan may need to be updated and re-tested more regularly.
Help during a response to a cyber incident is available from the NCSC via specialist CIR companies.

With thanks to Napier Meridian for their input to this document