ProtectUK

Tactic SB1: Establish or review a C-UAV/UAS Plan

ProtectUK publication date
14/12/2023

Information and Intention

There has been a significant growth in the legitimate use of Unmanned Aerial Systems (UAS) over recent years. This is anticipated to increase as the potential uses of UAS continue to develop. As this usage increases, security risks are also emerging.

An Unmanned Aerial Systems has 3 components:

- An unmanned aerial vehicle (UAV), commonly known as a drone;
- A Ground Control System (GCS) which allows the pilot to remotely control and/or monitor the operation of the UAV; and
- A bi-directional link between the UAV and the GCS which provides control, status and imagery information.

Drones can be used to achieve criminal or terrorist objectives. This can include disruption or endangerment to persons or property (including at airports or major events), intelligence, surveillance and hostile reconnaissance, as well as carrying out an attack by the delivery of dangerous payloads (e.g. improvised explosive devices). A hostile deploying a UAV over a sensitive, process-critical site such as an airport, can have a serious impact on operations within the site. The incident at Gatwick Airport in December 2018 highlighted the disruption that can be caused by a hostile UAV/UAS incident.

Consideration should be given by your organisation to establishing or reviewing a Counter-UAV/UAS (C-UAV/UAS) plan to ensure that your business or organisation can respond effectively to UAV-related security risks.

If there is a shared use of a site, the security and C-UAV/UAS plan may need to be adopted by multiple organisations. There are a number of reasons for this:

- Resources are effectively and efficiently used and there is no unnecessary duplication of effort.
- All incident reporting is assessed in a single location so that the richest assessment can be made.
- There is a rapid and coordinated response with no conflicting activity.
- Communication plans are coordinated to ensure a single and consistent message is released to the media and others.

Method

As C-UAV/UAS mitigations are considered, it is necessary to make sure that they link into existing security plans. This may involve adding the UAS related risks into the overarching site security risk assessment and updating the associated security strategy.

For further information on establishing and reviewing a C-UAV/UAS plan, see:

Countering threats from Unmanned Aerial Systems (C-UAS) | ProtectUK

Counter Uncrewed Aerial Systems - NPSA

Administration

Key decisions will need to be made at a senior level in the organisation as a plan is developed. It is important that senior decision-makers understand the UAV/UAS risks that have been identified and the options as to how they can be mitigated.

Early identification and engagement with internal and external stakeholders are important at each stage of the development of a Counter-UAV/UAS plan, from assessing the risk, through to developing appropriate responses. Agreement must be sought in relation to the roles and responsibilities of all those involved.

Engaging with the appropriate regulators should also be considered. Local organisations whose sites are nearby, or have shared use of the site being protected, are also likely to play an important part in developing and delivering the plan.
Further information on partner agency considerations and engagement can be found on the ProtectUK website: Countering threats from Unmanned Aerial Systems (C-UAS) | ProtectUK.

Risk Assessment

All activity relating to strategy should be risk-assessed in line with existing business/organisational

policies, including the site's strategic security risk assessment. This should include a high-level assessment of the security risks posed by UAV/UAS threats to the site and should involve an assessment of the threat, vulnerability and impact of a UAV/UAS incident. The risk assessment should be used to identify what mitigation the site needs to put in place.

Further information on the threat of drones in the UK can be found on the ProtectUK website: Threat from Drones in the UK - ProtectUK.

Additional information on risk assessment and considerations can be found on the ProtectUK website: Countering threats from Unmanned Aerial Systems (C-UAS) - ProtectUK.

A site vulnerability assessment for UAV/UAS threats should be completed, to inform the detailed risk assessment and the C-UAV/UAS plan. It will also provide information in relation to:

- The threat scenarios posed by UAV/UAS that are most relevant to a site.
- The type of UAV/UAS which might be used and how they may be used.
- The vulnerability of key assets.
- Where the likely launch points are situated.

Analysis should also be undertaken in relation to any historic UAV/UAS activity in and around the site. This will provide useful information as to what can be expected in relation to both UAV/UAS leisure use, but also any historic hostile use.

Communications

Early identification and engagement with internal and external stakeholders is important at each stage of the development of a C-UAV/UAS plan, from assessing the risk, through to developing appropriate responses. Agreement must be sought in relation to the roles and responsibilities of all those involved.

Internal Stakeholder Engagement:

In the event of a UAV incident at your site, it is essential that this information is communicated to the appropriate staff, and that they know what to do in such an eventuality.

Corporate communications should be developed and used to help:

- Deter potential malicious individuals from attempting to use UAV/UAS.
- Reassure the public and local community by promoting the efforts of the organisation and authorities to ensure their safety and security.
- Recruit the local community and the public to be part of the detection effort.

- Engage with all internal staff to increase their awareness of the threat from UAV/UAS.

Further information on security minded communications can be found on the ProtectUK website: Countering threats from Unmanned Aerial Systems (C-UAS) - ProtectUK.

You must provide information for your staff so that they can help deliver the plan. Your internal audience will inevitably cross over into your external audience, so you should consider the messages you want these individuals to communicate to their external networks e.g. families and friends. Remember that social media is a potential area where this crossover may occur.

External Stakeholder Engagement:

Early identification and engagement with key external stakeholders are important. Engaging with the appropriate regulators should also be considered. Local organisations whose sites are nearby, or have shared use of the site being protected, are also likely to play an important part in developing and delivering the plan, and consideration should be given to engaging with any working groups or forums who may already have identified ‘best practices’ and lessons learned from similar sites within the business area the site operates within.

There are a number of key principles that should be applied when engaging with stakeholders:

- The engagement should be different for different stakeholders, at different times – it should be flexible as one type of engagement process does not necessarily suit all stakeholders.
- It should be a two-way engagement process, where information and knowledge are shared.
- Communications should be genuine and timely, where there is the ability to influence outcomes, dependent on feedback.
- Engagement with stakeholders should be open and transparent.

As with all matters relating to security and policing, the relationships with the police are key. The contact may be with either the local police or those specifically tasked with providing policing to certain sites.

External Media Engagement:

After a UAV incident has occurred, organisations should avoid revealing details about the incident through social media without prior police consultation. An appropriate individual should be identified in the organisation to liaise with the police in order to disseminate approved information which is accurate, and which will not compromise any potential criminal investigation.

Health and Safety/Other Legal Issues

Businesses/organisations that are developing C-UAV/UAS plans should ensure that all activities are assessed in line with Health and Safety and other legal/policy frameworks, such as:

- The Human Rights Act 1998
- Health and Safety Acts
- Air Traffic Management and Unmanned Aircraft Act 2021
- Investigatory Powers Act 2016
- Wireless Telegraphy Act 2006
- Computer Misuse Act 1990
- The Data Protection Act 2018
- Employment Rights Act 1996

It is important to consider any responses to a UAV incident with regards to justification, proportionality, necessity and legality. Attempting to destroy or interfere with a UAV could lead to legal issues and all options should be considered, as potential mitigation measures in the risk assessment process.

You should ensure that there are well-defined governance arrangements and that records are kept relating to UAV related incidents. These include decisions made, and the reasoning behind those decisions. Records will provide evidence to any investigations, or public enquiries and assist in defending against legal action, criminal charges or civil claims.

KEYWORDS
UAV
DRONES
RISK ASSESSMENT
THREAT