Public Events UAS RIsk Framework

Public event managers need to be aware of risk assessment methodologies to detect threats, identify vulnerabilities, and reduce consequences. Information gathered through this process is extremely valuable for enhancing security measures.

Several risk assessment methodologies exist today. Whichever model your organization uses, drone risks can be integrated into your risk framework. As technology advances and threats evolve, your risk assessment needs to change as well.

Public or open access events include marathons, triathlons, golf tournaments, music festivals, outdoor festivals, fairs, etc. Public events face many of the same risks that stadiums and sports venues face. But unlike in stadiums, spectators and performers aren't concentrated in one area. Public events face the burden of securing a larger perimeter with continuously moving spectators.

Public events make an attractive target for both unintentional and intentional drone threats. Live events are an attractive target for criminals and terrorists, and attacks on lifestyle events carry a deep cultural significance. These venues also attract curious drone owners that want to capture a bird's-eye view of the event.

Soft targets chosen by terrorists share three important characteristics:

1) crowds of people
2) are easily accessible
3) can be surveilled without drawing too much attention to the potential attackers

In 2017, Homeland Security released a warning about the very real threat of drone attacks. As UAS proliferate, organizations should anticipate a rise in the types and number of such threats and prepare appropriately .

Identify the UAS Risks

The first step in preparing a UAS risk management plan is to identify potential risks drones pose to your organization. Understanding the scope of possible risks will help you develop realistic, cost-effective strategies for dealing with them.

Ways to identify UAS risks to your corporation:

During this step, consider these kinds of questions: “why?, what?, when?, where?, how?”

- Why would my event be threatened by a drone?

- What would happen if a drone hacked my venue?
- When will this happen, could it happen again?
- Where are my security gaps that would allow such an attack?
- How could my event be impacted by drones?

Brainstorm with different departments to gather a comprehensive view of drone risks, drone incidents will impact different areas of your organization. Discuss the types of questions above in your brainstorming session.

Use these questions to think about event-based scenarios that could happen during your event. Then establish which areas of your organization would be affected and the consequences of the event. Risk identification involves establishing three key concerns: sources of risk, areas of impact, and consequences.

Sources of UAS Risks/Threats:

As already stated, public events are an attractive target to both criminals and onlookers. As such, drone threats could originate from unintentional or targeted sources.

I. Unintentional: Negligent Drone Pilot (Hobbyist/Commercial)
II. Targeted: Domestic/International Terrorist, Nefarious Actor/"Lone wolf"

Areas of Impact:

If any of the risk events happened at your event, what areas of your organization would it influence? For instance consider the following - If a drone crashed on the crowd, would it: inflict human harm/casualties? cause a PR nightmare? lead to financial losses? lead to lawsuits?

Areas of Impacts to consider include: human injury/wellness, operational, financial, legal, and brand reputation.

Consequences

What would happen if a drone fell on or struck a participant at my event?

Research on drone-human collisions is a great concern to the FAA and other government entities. Research groups are studying these incidents to establish if it is safe for drones to fly above people. Research by various FAA supported groups have found that the likelihood of injury increased proportionally with the size of drone. Larger, heavier drones are more likely to cause more severe injuries.

Largest Injury Concern	Type of UAS Used	Typical Altitude and Forward Speed	Example Flight Scenario

Head and Shoulders	Quadcopters	High altitude, Low speed	Aerial Photography
Face and Torso	Quadcopters or Fixed Wing	Low altitude, High speed	Drone Racing
Lacerations	Quadcopters	Low Altitude, Low Speed	Concert Filming

Main injury categories:

1) Head and Shoulders
2) Face and Torso
3) Lacerations

There are three main types of injuries that can result from sUAS collision with a person.

1) **blunt force trauma** due to high energy impact on the body resulting in acceleration and shearing of organs or the uncontrolled movement of limbs due to impact.
2) **penetration injury**, which is associated with the application of large forces over small areas,
3) **laceration**, which is related to the application of large forces over small areas by propellers and rotors. Lacerations are also impacted by propeller blade leading edge sharpness and blade rigidity.

The severity of the human injury caused by a drone depends on:

1) **speed** of the drone
2) **altitude** the drone is flying
3) **type of drone**

Resources:
FAA's ASSURE: UAS Ground Collision Severity Evaluation Research
Virginia Tech's Institute for Critical Technology and Applied Science Drone-Human Collision Research

What would happen if a drone was used to drop biological/chemical agents onto the crowd?

This event is one of the worst-case scenarios, it would have significant impacts on human health/wellness, organization's finances, brand and reputation, and future ticket sales.

The task of arming a drone to carry a chemical agent is technically possible. Agricultural drones are equipped with chemical sprayers. Also chemical sprayer kits are available, which allow for easy drone modification.

What would happen if a drone armed with a bomb or other deadly device attacked my venue?

This is another worst-case scenario event that would have horrendous consequences, most likely severe injuries, casualties, and significant structural damages. The incident would impact many areas of the organization.

Consumer drones can be modified to carry and release a payload easily. In November of 2017, a California man modified his drone to drop leaflets over two stadiums while NFL games were taking place. Luckily the man was only releasing anti-media propaganda but it does highlight safety concerns, and it is easy to imagine a worse scenario.

Terrorists have already demonstrated their ability to attach an improvised explosive device (IED) to a drone.

Could these worst-case scenarios actually happen?

In November of 2017, Homeland Security released an updated terror bulletin that highlights the threat of weaponized drones, chemical attacks and the continued targeting of commercial planes.

During the U.S. Committee on Homeland Security and Governmental Affairs, Annual Threats to The Homeland Hearing, Nicholas Rasmussen, the director of the National Counterterrorism Center, spoke to a Senate panel about the growing threat and possibility of terrorists using drones to drop explosives or even unleash biological attacks on U.S. soil. Rasmussen, also told the committee, "A year ago this was an emerging problem. Now it's a real problem."

During the security committee briefing, FBI director remarks that terrorists have shown an interest using drone overseas and "the expectation is, it's coming here imminently." Drones are easy to acquire and operate, but they are difficult to disrupt and monitor. The briefing can be viewed on Youtube: FBI director discusses threats of terrorist drones.

Risk cannot be eliminated from the environment entirely, but with careful planning, it can be managed. Your organization may already have protocols for these types of worst-case scenarios, and the same procedures can be applied whether the threat is from a traditional perimeter breach or an aerial perimeter breach.

Analyze the Level of Risk

The next step is to identify the level of risk. The level of risk can best be understood as the probability of the event occurring and the product of the consequence of an event: Risk = Probability x Consequence.

Level of Risk = Probability x Consequence

The assessment of probability and consequence is somewhat subjective but subjectivity can be lessened by using data or facts collected from a range of available internal and external information.

Level of risk is often described as low, medium, high or very high. It should be analyzed in relation to what you are currently doing to control it. Keep in mind that control measures decrease the level of risk, but do not always eliminate it.

Probability

When determining the likelihood of an event or risk, it can seem hard to have a precise frequency. For instance, you may want to determine the frequency of drones operating near or above your event. First, you can ask personnel of all levels to report drone sighting and keep records of the events. This may not give you an exact number but can indicate if there is a problem, or if it's a growing concern.

Probability Scale

Level	Probability	Description
4	Very likely (frequent)	Has occurred 2-3 times in the past year
3	Likely (probable)	Occurred more than 4-5 times over 5 years in this organization or in other similar organizations; is known to have occurred in the past year
2	Unlikely (uncommon)	Has occurred 2 or 3 times over 10 years in this organization or similar organizations
1	Very unlikely (rare)	Has never happened in this industry

Consequence

Consequences will range from marginal/slight inconveniences to major/catastrophes. Determine how the events will impact different areas of your organization: will they affect human life, daily operations, information and technology, financial, marketing, brand & reputation, etc.

Consequence Scale

Level	Consequence	Areas of Impact		
		Human Injury	Business Operations	Financial
4	Severe	Death; human casualties	Complete shutdown of operation; halt core operations; major revenue loss	Severe financial loss; Significant budget overrun with no capacity to adjust within existing budget / resources
3	High	Multiple severe injuries	Shutdown of key operations; service delays, revenue loss	Major financial loss; Requires significant adjustment to approved / funded projects / programs / business activities
2	Moderate	Injuries may require hospitalization	Reduced performance may result in minor revenue loss; Organization existence is not threatened	Significant financial loss; Impact may be reduced by reallocating resources
1	Low	No human impact, minor injury	No impact to daily operations, Minimal impact on non-core operations.	Minor financial loss; Unlikely to impact budget or business activities

Note: Ratings vary for different types of organizations. The scales above use 4 different levels; however, you can use as many levels as you need. Also use descriptors that suit your purpose (e.g. you might measure consequences in terms of human health, dollar value, information loss).

Determine Risk Mitigation

Once you have established the level of risk, you then need to evaluate the risk and identify solutions. Risk mitigation involves determining what the acceptable and unacceptable risk levels are for your organization. It also involves identifying solutions or ways to treat the risks. Unacceptable risks range in severity; some risks will require immediate treatment while others can be monitored and treated later.

For example, you may decide the probability of a hobby drone pilot accidently crashing their drone into the crowd is 'likely' (a score of 3) but the consequences are 'moderate'' (a score of 2). Using the tables and formula above, this therefore has a risk rating of 6 (i.e. 3 x 2 = 6).

Risk rating table

Risk rating	Description	Action
12-16	Severe	Needs immediate corrective action
8-12	High	Needs corrective action within 1 month; monitor risk and re-evaluate at a later date
4-8	Moderate	Needs corrective action within 3 months; monitor risk and re-evaluate at a later date
1-4	Low	Does not currently require corrective action; monitor risk

Risks can be managed by one of four distinct methods: risk acceptance, risk avoidance, risk control (or reduction), and risk transfer (deflection).

Risk Management Strategies:

	Definition
Risk Acceptance	An explicit or implicit decision not to take an action that would affect a particular risk.
Risk Avoidance	A strategy or measure which effectively removes the exposure of an organization to a risk.
Risk Control (or reduction)	Deliberate actions taken to reduce a risk's potential for harm or maintain the risk at an acceptable level.
Risk Transfer (or deflection)	Shifting some or all of the risk to another entity, asset, system, network, or geographic areas.

Homeland Security: Risk Management Fundamentals (page 23)

Severe risks that cause a high degree of loss and occur frequently should be avoided at all costs. Minor risks with a low degree of loss may be acceptable. Not all the risk strategies can be implemented easily, discuss the best course of actions for your organization with your entire team.

Risk Acceptance:
Accept all risk of the event and consequences that come with the event occurring. Regarding drone risk, you accept the risk of human injury and the impacts it comes with, which could be financial, adverse impact on reputation,and legal liability.

Risk Avoidance:
By nature, public events are soft targets, and it is near impossible to avoid all risks. Event security personnel must harden perimeters and enhance security measures to keep the event as secure as possible to reduce the risks and severity of the threats.

Risk Control (Reduction):
Event managers can reduce risk through staff training, preventative maintenance, and development of a risk management plan as the standard operating procedure.
Communicate with all levels of employees the risk, from concession vendors to high-level managers; everyone needs to be aware of the dangers. If a concessions worker sees a drone, they need a procedure on who to tell; they need to be able to talk to those in the chain of command as well.

Event and security managers can access the risk, and if they determine it needs a more advanced solution, a drone detection system can integrate into existing security protocols.

Drone threats and risk impact the whole organization not just the security team, all teams can allocate or budget money to mitigate the costs. This will control the risk while reducing the financial burdens.

Risk Transfer (Deflection):
Sometimes managers will want to transfer the risk to someone else who is willing to assume the risk. For example if you hire or grant permission to drone operators for photography or videography, have the commercial drone operator assume the risks for human injury. Make sure you hire a company that carries insurance. Also require them to use propeller guards on their drone. Research shows propeller guards can reduce the severity of lacerations.

Risk assessment is an ongoing process. Whether you take action now or choose to monitor the situation, managers must re-evaluate risks on a continuous basis. Security perimeters are not just ground entry points, security and event managers need to consider the perimeters extending above the venue as well.