Infrastructure - UAS Risk Assessment Guideline

The risk environment affecting critical infrastructure is complex and uncertain; threats, vulnerabilities, and consequences have all evolved over the last 10 years. For example, as technology advances the types of attacks are evolving. Today's landscape of increased cyber and drone risks stems from growing integration of information and communications technologies with critical infrastructure operations and an adversary focus on exploiting potential cyber vulnerabilities.

Current drone law landscape

The Federal Aviation Administration (FAA) and Department of Energy (DOE) have agreed to restrict drone flights up to 400 feet within the lateral boundaries of seven Department of Energy (DOE) facilities. The FAA has placed similar airspace restrictions over military bases and assets. They have also prohibited drones usage over 10 Department of Interior facilities, which include several large dams and iconic landmarks.

Many states have set out to define critical infrastructures in their laws which seek to prohibit drones from flying over or near these facilities. Currently, 10 states specifically restrict drone access near critical facilities and infrastructures

The Department of Homeland Security identifies 16 critical infrastructure sectors:

Critical infrastructure risks can be assessed in terms of the following:

- Threat – natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- Vulnerability – physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
- Consequence – effect of an event, incident, or occurrence.

1. Identify UAS Risk

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

- Why would my facility be targeted by a drone?
- What would happen if a drone hacked my facility?
- When will this happen, could it happen again?

- Where are my security gaps that would allow such an attack?
- How could my facility be impacted by drones?

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

Sources of Risk

The Department of Homeland Security (DHS) Risk Lexicon, defines a threat as "a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property." Drone threats are a risk that critical infrastructures face and left untreated can pose problems to national security.

The risks associated with drones are mainly external. External drone threats to critical infrastructure and facilities could originate from unintentional or targeted sources.

1. Unintentional: Negligent Drone Pilot
2. Targeted: Domestic/International Terrorist, Hacker, Nefarious Actor/”Lone wolf”

Areas of Impact

Critical infrastructures have many areas of impact to consider when identifying risks. Areas of impact to consider include: human life, operations, service delivery, financial, legal concerns, and brand/reputation.

Consequences

Brainstorm with a team, include various levels of employees that work in the different areas of impact. Think about all consequences - ranging from a mild inconvenience to a worst-case scenario.

Security experts have warned that drones could be used by terrorists to surveil or assist in carrying out an attack on critical infrastructure and critical facilities.

The FBI and DHS have warned about attacks on the nation's critical infrastructures. Late 2017, agencies released a joint statement, warning about recurring cyber attacks to critical infrastructures and their partners. With the United States aging infrastructure, an attack to out power grid or other sensitive facilities could have devastating consequences and the effects could easy domino into all areas of life.

What would happen if a drone attacked a critical infrastructure?

International or homegrown terrorists could adapt and refine the tactics they use in conflict zone like portable unmanned aerial systems or drones with explosives to attack key facilities, the ability to attach an improvised explosive device (IED) to a drone has already been demonstrated by terrorists.

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.

Video can be watched on Youtube: FBI director discusses threats of terrorist drones. To watch the entire committee hearing, click the link: Threats to the Homeland Committee Hearing Video.

What would happen if a drone was used to hack the power grid?

A cyberattack against the United States' power grid could cost as much as $1 trillion to the U.S. economy, according to a report published in 2015 from the University of Cambridge Centre for Risk Studies and the Lloyd's of London insurance market.

Experts predict this scenario would result in a rise in mortality rates as health and safety systems fail; a decline in trade as ports shut down; disruption to water supplies as electric pumps fail and chaos to transport networks as infrastructure collapses.

The total impact to the U.S. economy is estimated at $243 billion, but economic losses could top $1 trillion in the most extreme version of the scenario.

Lloyd's of London: Whitepaper - Implications of attack on us power grid https://www.insurancejournal.com/research/research/business-blackout-lloyds-report-on-implications-of-attack-on-u-s-power-grid/

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

2. 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.

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 company. First, you can ask employees 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.

Another way to determine the frequency of drone sightings is to monitor drones with drone detection technology. Reputable companies will allow you to try out or rent drone detection equipment for a trial period (30-day or 60-day trial), this will give the most accurate numbers to access the actual probability.

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: daily operations, information and technology, financial, marketing and PR, human/public/national safety.

Consequence Scale

		Areas of Impact		
Level	**Consequence**	**Operations**	**Financial**	**Human/Safety**
4	Severe	Complete shutdown of operation; halt core operations;	Severe financial loss; Significant budget overrun with no capacity to adjust existing budget/resources	Death(s)/compromises to national security
3	High	Shutdown of key operations; service delays	Major financial loss; Requires significant adjustment to budgets	Severe injuries, sickness. Compromises public safety
2	Moderate	Reduced performance may result in minor revenue loss; Organization existence is not threatened	Significant financial loss; Impact may be reduced by reallocating resources	Minor injuries, non life-threatening compromise to public

1	Low	No impact to daily operations, Minimal impact on non-core operations.	Minor financial loss; Unlikely to impact budget or business activities	Little actual impact to public or national security; no injuries

Note: Ratings vary for different types of critical infrastructures. The scales above use 4 different levels; however, the number of levels can be adjusted to meet the organization's need. Also use descriptors that suit your purpose (e.g. you might measure consequences in terms of human health, dollar value, information loss, time loss).

3. Determine Risk Mitigation

Once the level of risk is established, analyze 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 solutions while others can be monitored and treated later.

For example, you may decide the probability of a drone used to survey critical infrastructure structure is 'likely' (a score of 3) and the consequences are 'moderate' (a score of 2). Using the tables and formula above, a "drone surveying critical infrastructure perimeter security" has a risk rating of 9 (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

4. Risk Management Strategies

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

	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.

Source: Homeland Security: Risk Management Fundamentals (page 23)

It is up to owners and stakeholders to determine what risk level is acceptable and unacceptable. 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 risks of a cyber or physical drone attack and the impacts it comes with, which could be financial, adverse impact on reputation,and legal liability.

Risk Avoidance

How might you remove your venue from exposure to a drone hacking your company’s information? It is almost impossible to remove a building or facility with outside exposure from aerial threats completely.

Risk Control (Reduction)

Facility 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 maintenance workers to high-level managers; everyone needs to be aware of the dangers. If a roof air conditioner maintenance worker sees a drone on the roof, they need a procedure on who to tell; they need to be able to talk to those in the chain of command to report the incident.

Facility and operations managers can assess the risk, and if they determine it needs a more advanced solution, a drone detection system can integrate into existing security protocols. As stated before, reputable companies will allow you to set up drone detection systems on a trial basis before investing in an expensive system.

Drone threats and risks impact the whole organization not just one 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. Insurance is the most applicable way to transfer risk.

Conclusion

Risk management is an ongoing process. Whether you take action now or choose to monitor the situation for an extended period, decision makers must re-evaluate threats, vulnerabilities, or potential consequences on a continuous basis. With rapidly changing technology and new exploits, critical infrastructures must prepare to reduce security gaps and evolve their physical security standards.