Kittyhawk

Factors, Tactics and Methods for Securing UAS Operations

Secure is a relative term.

In aviation, we talk about risk not as if something will happen or not, but the amount of time it will take something to happen. As much flying as there is in the world, it's a matter not of if but of when there will be an accident. This is never more evident than when you hear safety professionals talking about airline safety. The United States, the gold standard of airline safety in the world, has a safety standard of "10^9" (hours of flying to be involved in a fatal airliner accident.) You'll also see this type of risk evaluation use in the medical field. When a drug says it's 91% effective, they're really saying that 9 out of 100 people continue to experience their symptoms.

Luckily, with computer security, we often have more control of our domain since computer code executes the same way, doesn't fatigue, and the chips running our computers don't have bad days the way humans do. But it's still helpful to think about risk in the same way: It's not a matter of if, but when. Our job as professionals is to weigh opportunity and security to reduce the likelihood of a security event and to minimize the impact it has on our organizations.

Given that we're approaching secure as a relative term, we'll need to look inward and assess what we're protecting, who we're protecting it from, and the amount of compromise in our own convenience, we're willing to accept for our **security posture**.

Like safety, security isn't a checkbox. It's an ongoing process that requires effort, resources and buy-in from all of the stakeholders involved. Done properly, your team can operate efficiently while still maintaining an excellent hold over your data and keeping it away from prying eyes.

What is a security posture?

A security posture is the full picture of your ability to mitigate and respond to threats. This includes everything from hardware, software, telephones, routers, cloud providers, and drone hardware providers. A security posture is the full operating picture you'll be working with. It also includes your processes for handling security as well as your readiness to respond, react, and mitigate events related to your security.

PART 1:

Do A Risk Assessment

As drone industry members, we're all hopefully familiar with the concept of a risk assessment. A risk assessment is an honest look at the operating picture and the risks around it. There are no wrong answers.

We need to perform a risk assessment of our drone program to understand the kinds of data we're trying to collect, where it will be used, how it will be moved around and who will have access to it.

There are a number of different ways you can do a risk assessment for your security posture. In general, every good assessment should have 4 phases: plan & identify stakeholders, review, report and strengthen. For demonstration purposes here, we'll be doing an example risk assessment of a utility company that has different classes of assets with different security requirements.

IDENTIFY STAKEHOLDERS

In many organizations, there are IT stakeholders you'll want to involve since they may have a more complete operating picture than just the drone team.

Acme Electric Netsec/Drone Stakeholders

- Director IT Security
- Chief Pilot (Crewed aviation program)
- Software Vendors' Key Stakeholders (Someone with Security or C in their title)
- GIS Director

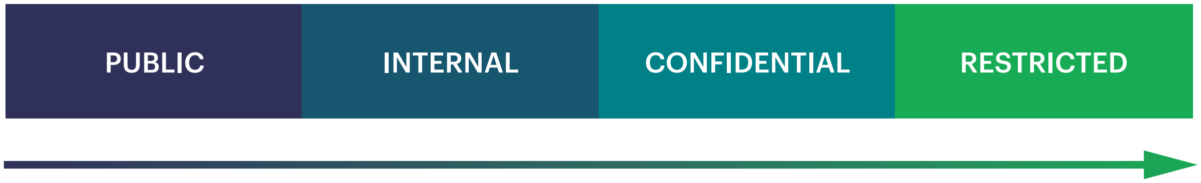
CLASSIFY THE DATA YOU'LL BE COLLECTING

Data classification is the process of segmenting your data into different categories of sensitivity. This will help you identify the lengths you'll need to go to protect that data. For example, some of your data will likely be ok to be *logically separated,* but other data may need to be *physically separated.* Some of your data may be so sensitive that it needs to be *ephemeral* or immediately destroyed after using. This classification process will help you come up with *data handling procedures* and a sensible *data retention policy.*

Below, you can find an example of a data classification matrix that might help. In general, it's a best practice to keep data classification into 3-4 "big buckets". Adding too many choices can create mis-classification due to confusion, or potentially worse, highly polarized buckets because when in doubt, employees choose more aggressive choices—leaving you with 80% of your data classified in 3-4 categories and 20% of your data scattered across the remaining categories. This is a logistical and security nightmare since it introduces too much discretion and thus, potential data leakage among the categories. For example, one employee might classify something as Confidential and another may classify the same data as Restricted. If the employee is wrong about it being classified, and it needs to be restricted, serious implications can happen. The fewer categories you have, the less chance of this scenario happening.

For our example, Acme Electric uses 4 classifications:

- Public
- Internal
- Confidential
- Restricted



Severity of Information Leakage Impact

Note: *The X scale of any classification you use should be about the impact of that data reaching an audience it shouldn't.*

Classification Types

PUBLIC

Any information that's available to the general public. For drone programs, you have to think outside of the company box a little bit. Since external data-holders like regulators are involved, you have to be cognizant of what they may be publishing. Whether that's a 333 Exemption, a COA, or a waiver.

For example, Kittyhawk's night waiver includes key stakeholders' names and our company office address. If your drone program is of a highly proprietary nature, the existence of a waiver alone (i.e., BVLOS, Flights over people, large drones, etc) could be a data leak in and of itself.

INTERNAL

Most companies classify things like memos, emails, and organizational charts as "Internal." Obviously, titles are public but understanding who reports to whom can be valuable information for an attacker looking to exploit organizational weaknesses, or perhaps less maliciously, salespeople looking for the right decision maker.

CONFIDENTIAL

This would be information that should never be public, and in some cases, may be not available to other people inside of the organization. An example of this might be customer information, customer leads pipeline data, or employee pay stubs. You might think of this classification as available to many, but not all in the organization.

RESTRICTED

This is information that would have a severe and material impact on the organization and potentially the rest of the world if it were released. Examples of this in Acme Electric might be internal pictures of certain power generation facilities with DOE oversight. Other good examples might include earnings reports, product roadmaps, or proprietary source code. This classification can be thought of as available to a few in an organization, and likely has tracked access.

Acme Electric Data Types & Classifications

DATA TYPE	STORED/MANAGED BY	CLASSIFICATION
Drone Reg #	FAA/Acme/Vendor	Public
Drone Telemetry (Location, Time, Operator, etc)	Acme/Vendor	Internal or Public (Someone could see you flying a drone at x spot at y time.)
Sensor images for map making	Acme/Vendor (Optional)	Internal (Since aerial mapping is available at lower resolutions, we can keep this as internal)
Inspection images of proprietary equipment	Acme/Vendor	Classified (IP, like Flare Stacks etc, should be Classified per our chart above)
Internal facility images	Acme	Restricted (Only available to a few in the organization, highly regulated, catastrophic if leaked)
Sensor video	Acme/Vendor	Internal
Live streaming / Emergency live streaming	Vendor	Restricted (Only to EOC, key stakeholders, and only for real time decision making. No need to risk a leak to the news, investors, etc)

ASIDE: CREDENTIALS

In addition to the data you'll be collecting, you'll also want to think about how you're going to handle credentials. This could be how your team accesses your data, or the way in which you interact with various services that store and process it.

For third party services, it's highly preferable to use a federated or "Single Sign-On" system. This allows your team to centralize all your user management. If an employee is dismissed, once their work credentials are revoked, all their third party credentials also cease to function.

Aside from usernames and passwords, use a proper credential management system, whether it's a system with levels and secure storage like 1Password or something more enterprise focused like AWS Secrets Manager.

In addition, you'll want to make someone a stakeholder in charge of managing all of this. While seemingly obvious, there have been some high-profile examples of credentials making their way out into the public eye.

PART 2:

Determining Your Potential Adversaries

Just like we have different types of data that we need to protect differently, we also have different potential adversaries that require different types of mitigation for the risks they pose. A large activist group is going to have different objectives than a curious teenager, and they'll both have different objectives than a nation-state.

Depending on your industry, type of data collected, and the methods with which you utilize that data, you could have different adversaries. This is a good time to take a look at your dataset and classification and remind yourself and the team that you can't steal what you don't have. Drones are terrific little generators of data, but much like a new puppy, you'll have to feed and care for that data for the entirety of its lifetime. Selecting what to keep can make you far less interesting to adversaries.

If you can harken to the proliferation of home security systems and their terrible commercials in the 1990's: A burglar is prowling the neighborhood only to see a "Protected by Home Security Company" sign in the front yard and decides to keep on prowling. If you can diminish the reward and maximize the effort enough, it suddenly makes your drone program a lot less of an interesting target.

As part of this, you should take a look with your whole team about your potential adversaries and be as critical as you can. For example, there was a serious drone security breach that affected law enforcement. In this case, it wasn't just criminals that might be interested but you'd also want to include anti-law enforcement groups, security researchers, and the like. Their data would all likely be classified as Confidential because of who their customers are, and who the adversaries of their customers are.

When it comes to adversaries, the easiest way to classify them is with four metrics: Time, People, Information and Money. Though you can often trade one for the other three, you'll most often need some combination of them to execute successful attacks on your program.

Understanding Your Adversaries

Understanding your data collection and compliance lets you more sensibly assess your risk.

Curious Teenager
No $$$

Ex-Employee
Insider info

Activists
Lots of people

Competing Company
Lots of $$$
and people

Nation State
Most $$$
and people

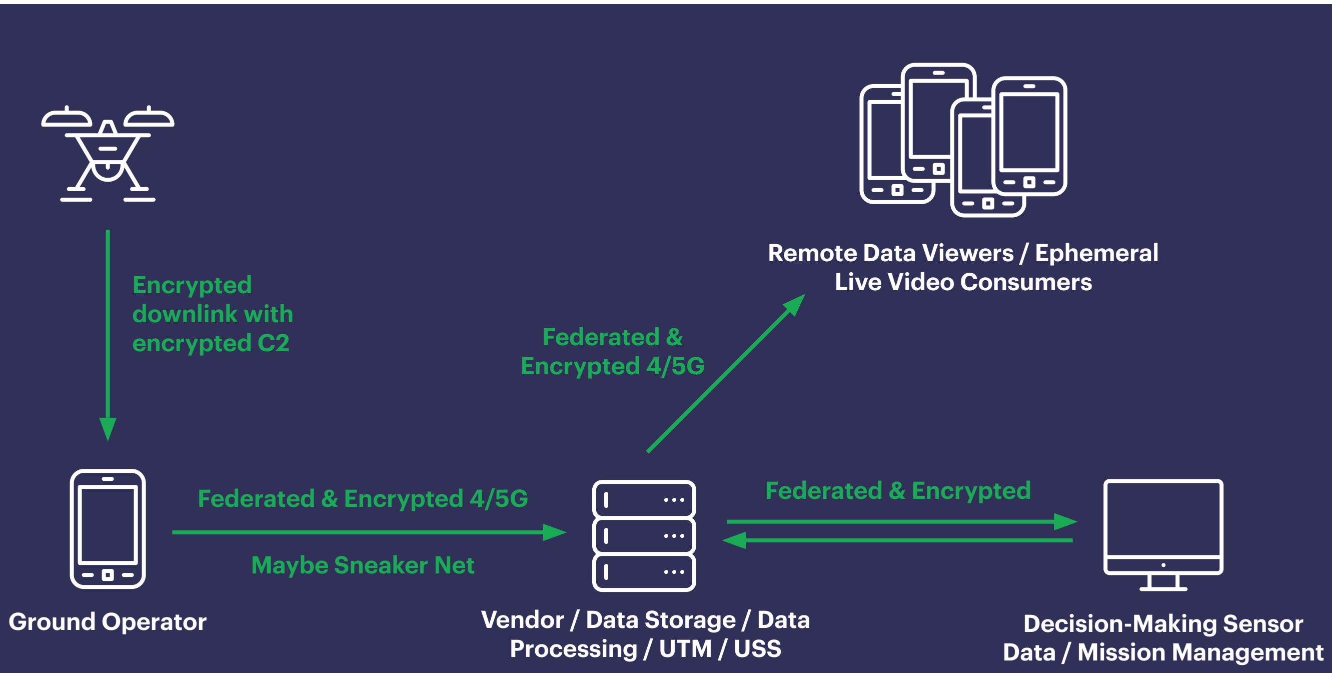
PART 3:

Assessing Your Operating Picture

MAKE A DATA FLOW DIAGRAM

Once you've determined all of the data that you'll be collecting and have solid ideas on how you're classifying it, you can move forward with how that data is going to move through both vendor systems and internal systems.

For this, it's often helpful to create diagrams that help explain the flow of data so stakeholders are able to more easily understand what systems are going to be involved and the paths that data is going to take to and from those systems. If you've never made a data-flow diagram, there are several helpful tools that make it easy. Lucid Chart is our favorite here at Kittyhawk.


Remote Data Viewers / Ephemeral Live Video Consumers
Encrypted downlink with encrypted C2
Federated & Encrypted 4/5G
Federated & Encrypted 4/5G
Maybe Sneaker Net
Federated & Encrypted
Ground Operator
Vendor / Data Storage / Data Processing / UTM / USS
Decision-Making Sensor Data / Mission Management

At Kittyhawk, we strive to make sure that every step of the data flow diagram is encrypted. The fewer opportunities for data to "run free", the fewer opportunities for someone to accidentally or intentionally become privy to it.

PART 4:

Information is Power: Operational Security Suggestions

Now, your organization is armed with the information you need to make good decisions about caring for your data. Hopefully, you'll have all the stakeholders you need involved, and you'll all be sharing the same common operating picture using a standard nomenclature.

In the last part of this document, we want to share some operational security information that can help bring a practical slant to some of the concepts we talked about above.

EXIF META DATA

When your drone takes pictures, it encodes all manner of additional information inside of the picture file. This data isn't just put there to make drones a spying tool. In fact, your phone camera likely does the same thing. It can be used for processing many pictures into a larger, more complete picture using photogrammetry. This data is also how Apple can show you a map with all your pictures on it, or group your pictures together with names like, "Your Trip To Reno."

Unfortunately, this data can also be used for nefarious purposes. It's been used to "doxx" unsuspecting teenagers posting selfies to the Internet, and it can be used by your adversaries. Obviously the location data is extremely important but there are second order effects as well. For example, if you bought the WhizBang 4000 drone and it had a critical security flaw in it, that's very sensitive information. If every picture you've ever taken at your company has data embedded in it that says, "Taken by WhizBang 4000", that could make you a more juicy target for attack.

There are various tools available online and for download that allow you to remove the EXIF data from your pictures.

THINK CAREFULLY BEFORE ANSWERING IN THE "DEFAULT"

A lot of third parties will want your information to register for various services. It's easy to register as Your. Name@YourCompany.com This is a terrific form of data leakage. It correlates hardware and/or software to your organization, and even gives additional information about who might be using and operating it. A primary early tactic that adversaries will use is trying to gather as much information about your organization as possible in order to correlate the equipment and software you use with publicly, or in the case of well funded nations or organizations, perhaps private exploits to gain access. Anytime you have the opportunity to deny information to potential adversaries, it's likely a good idea to do so. If vendor x has a data breach, and the attackers are able to abscond with a customer list, a myriad of malicious actors now know that at the very least, this software or hardware once existed in your organization. It doesn't even have to be publicly accessible.

Take Adobe Acrobat Reader for example. It's virtually universal in the business world. However, it's been plagued with a range of security problems and many of them are able to be exploited by *just opening* a PDF document. Now consider how many different file types exist in your drone program, and the number of people in your drone program who despite training and their best intentions may not find it suspicious to open one of these file types when it's got a small message prepending it like, "This didn't measure right for me. Can you take a look?"

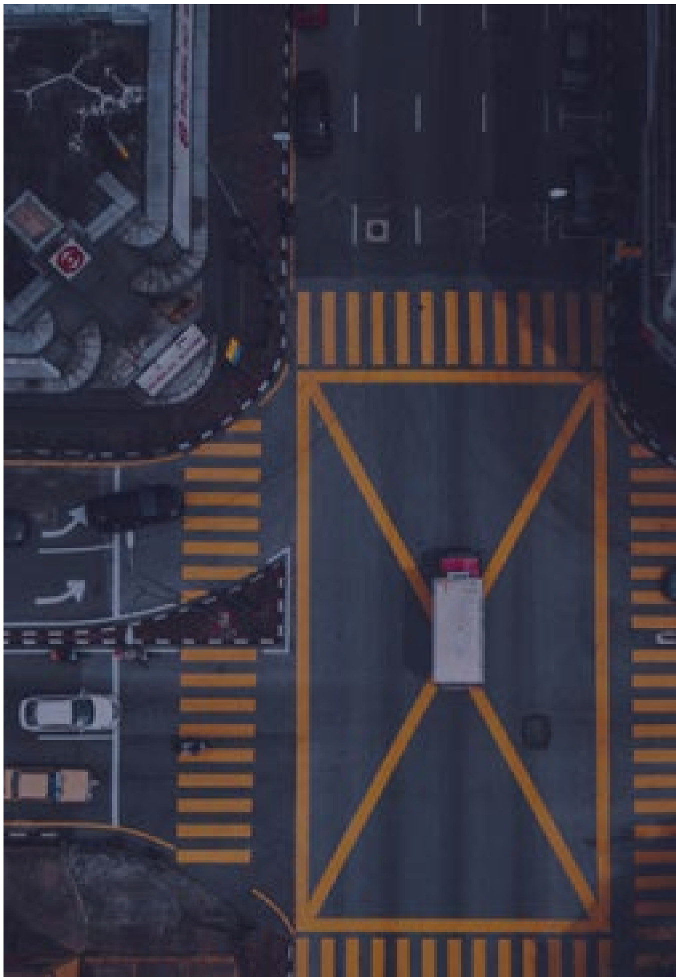
When in doubt, use your credential management system to create dedicated emails. These can be paid or free but Drone23851@Yahoo.com isn't even in the same order of magnitude as useful to an adversary as Your.Name@YourCompany.com

WORK WITH TRUSTED VENDORS

Just because a company is big or popular doesn't mean they take your security very seriously. You can type "Data breach" into Google News and see daily stories of companies that didn't value their data and their adversaries correctly.

One key thing you can look for is third party validation. This can come in many forms but there are two key types that are important to note. The first is practical evaluations. Are they undergoing code reviews in the Software Development Lifecycle (SDLC)? Are they using tools to verify the quality of their work? But also, are they putting their hypothetical quality to the test against real adversaries?

Companies will frequently work with "Red teams", or groups of skilled hackers that have agreed not to break or disclose anything if they are able to gain access to the system. These penetration tests provide real world validation that the processes and procedures for development are working well. Never hesitate to ask if a vendor has the latest copy of their penetration and remediation workflows.



Having hackers come in and raise havoc hopefully doesn't yield a lot of problems because of the processes in place. You should consult with your stakeholders, mentioned at the beginning of this document, to determine what your team prefers. There are a number of ways you can assess the processes they include but certainly aren't limited to:

1. SOC 2 Type 1 and SOC 2 Type 2
2. ISO 270001
3. FIPS (Most commonly used by government and their contractors)

An interesting benefit to SOC 2 is that vendors are required to keep a list of OTHER vendors they work with and the kinds of data they hold, and the kinds of security they employ.

SINGLE SIGN-ON (SSO)

Drones lend themselves to using a lot of different platforms and vendors. With each additional user in your organization, your complexity of managing your organization grows. When you combine that with requirements from your stakeholders like password hygiene, it can become a full time job managing this minutia.

Luckily, with Single Sign-On integrations, you can manage all of this at a corporate level. A SAML or oAuth2 integration allows you to control all of the users, their access to third party platforms, as well as enforce all of your password change and complexity requirements.

Any vendor that doesn't offer SSO should at the very least have mitigations in place to inhibit brute force attacks. This may look like "**login throttling**" or 2 factor authentication. But ideally, you're using and enforcing those on a corporate level using Single Sign-On rather than a vendor's.

What is login throttling?

A programmatic way to decrease the number of possible login attempts over time in order to thwart brute force attacks that quickly try lots of username and password combinations.

ALLOW AND DENY LISTS

Network security has long made use of allow and deny lists. Today, they can take a lot of different forms so it's worth reviewing some of the ways you might utilize them.

- **Geographical Allow and Deny Lists** – In particular, Kittyhawk has seen the utility of this first-hand with some of our more national security minded customers. They have certain mandates that data not pass through certain countries. Setting up some common sense geographical deny lists can keep out bad actors that may not specifically be targeting your organization and operate in more of a "drive-by" fashion.

  As with all things in security, this isn't fool-proof and won't cure all. We're not trying to use one method to protect against everything, we want to create layers of security to make it more difficult for attackers.

- **IP Based Allow and Deny Lists** – This is one of the most extreme versions of the allow and deny list. It often requires you to have fixed *IP addresses*. This means it won't work with devices that move about different networks with different IPs. You can imagine IP addresses like telephone numbers and this Allow and Deny List like the ability to put a list of phone numbers in your phone that will make it ring. Everyone else will hear "The number you have dialed is not in service..." This type of allow and deny works well for building a "direct link" between two places. Oftentimes at Kittyhawk, we will see implementations of this to fixed areas like Emergency Operation Centers. This is a great way to make sure that critical data isn't wandering anywhere it shouldn't. Another bonus is you'll have a very narrow list of people accessing it.
- **Devices/Agents** – If you know that your team only uses certain types of hardware or software, it can make sense to add in additional protections here. If you know that your entire team only flies with a particular Android phone, it might make sense to put any iOS device on a deny list.

PART 5:

Creating a Security Culture.
(Hint: You've seen this movie before)

One thing we've been consistently impressed with over the years at Kittyhawk is how seriously our customers take safety. They are vigilant in creating a safety culture. Moreover, they don't just talk the talk, but they walk the walk. For example, one safety program has a policy that anyone is allowed to issue a "stop work" at any time. This means it could be your first day at the most entry level position and if you see something amiss safety wise, you can shut down the whole worksite.

While it is probably not generally advisable to have first day employees running around turning off routers, computers and slamming laptops shut, there is a good precedent to learn from. For example, if your operational security means not using certain apps on work phones due to security threats, then you must be willing to tolerate employees strictly following that policy. It may be more costly when they come back unable to do a particular job because they needed a certain functionality, but you must ask yourself what is security worth to you?

A much more scary scenario is that an employee fires up their personal phone, installs the banned application, and then takes company data to their personal device while also giving data to this banned application. This can easily be a nightmare scenario.

Creating a process by which employees can report security problems, concerns, and the like, without penalty, is key to creating a security culture. You may even say that amnesty will be given provided security related concerns are reported but will not offer amnesty if they're not.

NASA and the FAA have used a methodology similar to this with great success. If a certificated pilot has an incident in which they broke the rules, they can go to the Aviation Safety Reporting System and document what went wrong and it will be non-punitive.

A simple form or email like SecurityConcerns@Company.com can become your first line of defense if something seems amiss.

Of course, you'll also want to pair this with training to help employees identify the things they want to report. This could be data leakage, unsanctioned software usage, or "spear phishing" attempts against them. Your key to good data coming from your whistleblower process will be educating your team as to what they should be flagging for further examination.

IN CONCLUSION

There is no conclusion.

Security is not a product you can buy. It's not a plugin. It's not a switch you can flip. Security is a process that requires ongoing vigilance to work. It requires transparency both inside of your organization and with your vendors about what everyone is doing at any given time.

If you can take away any one thing from this document, it would be that good security more closely resembles a labyrinth than it does a very high wall. We want potential attackers to have to try and circumvent many different types and layers of security, each one of which could and should alert us to malicious activity and give us a chance to mitigate their attacks.

Kittyhawk

Kittyhawk is a leading enterprise software platform for drones. Kittyhawk powers a platform that helps enterprise drone programs to operate and scale, comply with regulations, and fly safely. Enterprise drone programs - from small teams to large corporate operations with hundreds of licensed drone operators - use the Kittyhawk platform every day.

Kittyhawk is a member of the FAA's Unmanned Aircraft Safety Team, the ASTM F38 committee on Remote ID, and a participant in the InterUSS project. We are also an FAA-approved USS for the LAANC program, which enables on-demand airspace authorizations in controlled airspace, and the provider of the FAA's B4UFly app.

To learn more about Kittyhawk, visit www.kittyhawk.io and follow us on Twitter @KittyhawkIO