Corporate UAS Risk Framework

Corporations face many threats that impact business operations. One emerging threat of great concern comes from unmanned aircraft systems (UAS) or also known as drones. From cyber threats to corporate espionage, drones present corporations with unique challenges.

Identify Corporate UAS Risk

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:

Consider these kinds of questions: “why?, what?, when?, where?, how?”

- Why would my organization be threatened by a drone?
- What would happen if a drone hacked my company?
- When will this happen, could it happen again?
- Where are my security gaps that would allow such an attack?
- How could my business 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. For instance consider the following - Will a drone cyber attack: disrupt your daily business activities? cause a PR nightmare? lead to financial losses?

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

Sources of UAS Corporate Risks/Threats:

I. Internal: Third-parties: including suppliers, consultants and contractors, and employees
II. External: Hacker, Cyber criminal, Former employee, Former third-party, Competitor
III. External: Amateur drone pilot (hobbyist)

According to PwC’s information security survey, current employees remain the top source of security incidents. From 2016 to 2017, Incidents attributed to hackers, competitors and other outsiders declined slightly. However, those attributed to insiders, such as third parties—

including suppliers, consultants and contractors—and employees, have remained about the same or increased.

Some incidents could originate from an amateur drone pilot (hobbyist) wanting to film the construction of your new corporate campus or record a meeting. Then they release the video on social media, inadvertently releasing sensitive and private information.

Areas of Impact:

Areas of Impact will differ depending on your industry or type of business. Areas of impact to consider include: Operations, IT, Financial, Legal, Marketing, and Public Relations.

Consequences

Brand and Company Reputation
A cyber attack can not only expose the company's data to hackers, but also customer's data. A company must handle customer's data with care. Due to many security breaches among big name companies, the public's confidence in company's acting responsible with data is at low. In According to PwC's 2017 US Consumer Intelligence Series survey, only 25% of consumers say they believe most companies handle sensitive personal data responsibly. Data breaches and leaks have a very negative impact on brand and company reputation.

Cost of Cyber Attack
In 2017, the average cost of a data breach in North America is $1.3 million for enterprises and $117,000 for small and medium-sized businesses (SMBs).

Globally, the cost of a data breach for enterprises has risen 11 percent in 2017. In the U.S., the average cost of a cyber attack for enterprises grew from $1.2 million in 2016 to $1.3 million in 2017. That's 10 times higher than the $117K cost of a breach for SMBs.

Overall, businesses are looking at IT security as more of an investment in 2017. In fact, IT security budgets are up, reaching 18 percent for enterprises compared to 16 percent in 2016. Even small businesses with fewer resources are investing more in IT security budgets this year — 14 percent compared to 13 percent in 2016.

In North America, the Kaspersky Lab study found that the following incidents had the most severe financial impact in 2017:

Financial impact on enterprises

1. Physical loss of devices or media containing data ($2.8 million)
2. Incidents affecting IT infrastructure hosted by a third party ($2.2 million)
3. Electronic leakage of data ($1.9 million)
4. Inappropriate IT resource use by employees ($1.1 million)

5. Viruses and malware ($519,000)

Financial impact on SMBs

1. Targeted attacks ($188,000)
2. Incidents involving non-computing connected devices ($152,000)
3. Physical loss of devices or media containing data ($83,000)
4. Inappropriate IT resource use by employees ($79,000)
5. Viruses and malware ($68,000)

The top “pain points” with the largest average costs after a breach for enterprises include $207,000 for internal staff wages, $172,000 for improved software/infrastructure, and $153,000 spent on cybersecurity training.

The top pain points for SMBs in 2017 include $21,000 in lost business and another $21,000 in costs related to employing external professionals.

Resources:
PwC Report: Key findings from The Global State of Information Security® Survey 2018
CSO Article - Kaspersky Lab Report: Cyber attacks cost U.S. enterprises $1.3 million on average in 2017

Could a drone hack my company?

Drones can be used for surveillance and corporate espionage. Drones can gather competitive intelligence by spying on meetings, mapping location layouts, and monitoring the pattern of your security personnel movements.

With a little modification, a drone can provide high tech corporate espionage. There have been reports of drones equipped with a Raspberry Pi or Wi-Fi Pineapple that landed on the roof of a data center and stole sensitive information. This is a common hacker practice, known as “rooftop packet sniffing.”

A drone can carry a lightweight yet powerful hacking platform such as a Raspberry Pi or Wi-Fi Pineapple, packaged with an external battery pack and cellular connection, for eavesdropping and man-in-the-middle (MITM) attacks. Even if the drone’s battery dies, the hacking platform will still transmit the data collected. Wireless printers are often the weak link in a company’s wireless network. A wireless printer’s connection is typically open by default; the open connection provides an access point for outsiders to connect to a business’s network and siphon information.

By attaching a Raspberry Pi, loaded with all the most common hacking software, to a drone you have a flying hacker laptop. Danger Drone was a proof-of-concept that debuted in 2016 as a pentesting tool. The danger drone can easily be cloned for malicious purposes.

Resources:
Hacking capabilities of drones
Motherboard: How a Wi-Fi Pineapple can steal your data
Motherboard: The 'Danger Drone' Is a $500 Flying Hacker Laptop

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 can be more quantitative 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.

Consequence Scale

Level	Consequence	Areas of Impact		
		Business Operations	Financial	Brand/Reputation
4	Severe	Complete shutdown of operation; halt core operations; major revenue loss	Severe financial loss; Significant budget overrun with no capacity to adjust existing budget/resources	Loss in customer loyalty; failure to gain new customers; Major PR campaign expenses
3	High	Shutdown of key operations; service delays, revenue loss	Major financial loss; Requires significant adjustment to budgets	Loss in customer confidence; Moderate PR campaign expenses
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	Slight loss in customer loyalty; expand PR campaign budget to lessen blow to company image
1	Low	No impact to daily operations, Minimal impact on non-core operations.	Minor financial loss; Unlikely to impact budget or business activities	Little to no impact on customer loyalty

Note: Ratings vary for different types of businesses. 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 solutions while others can be monitored and treated later.

For example, you may decide the probability of a former employee using a drone to hack your company is 'likely' (a score of 3) and the consequences are 'high' (a score of 3). Using the tables and formula above, a “former employee cyber drone hack” therefore has a risk rating of 9 (i.e. 3 x 3 = 9).

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)

It is up to owners and business partners to determine what risk 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 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 company from exposure to a drone hacking your company's information? In today's connected world that relies on computers, it is impossible to remove the threat of any kind of cyber attack. You could remove aspects of your business from some types of corporate espionage, such as conducting secret meetings.

Risk Control (Reduction):
IT managers can reduce risk through staff training, preventative security measures, 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 an 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.

Business and IT 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. As stated before, reputable companies will allow you to set up drone detection systems on a trial basis before investing in an expensive system you don't need yet.

Drone threats and risk impact the whole organization not just the IT 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.

Risk management is an ongoing process. Whether you take action now or choose to monitor the situation, business decision makers must re-evaluate risks on a continuous basis. Security breaches typically take place from computers in various locations, but sometimes it can happen from right over your head. With rapidly changing technology and new cyber exploits, IT and security managers face a constant battle of thwarting cyber attacks.