The CIA triad is the cornerstone of cybersecurity policy. When applied in the context of securing an asset, they can broadly be described as follows. Confidentiality can be thought of as similar to privacy. It is the act of preventing sensitive assets from being accessed or viewed by unauthorized parties. Integrity is the prevention of unauthorized manipulation of assets. The goal of integrity is to maintain the consistency, accuracy, and ultimately the trustworthiness of the asset. Finally, availability is the idea that critical assets should be able to be utilized by authorized parties when they are needed. When taken together, these three pillars provide a comprehensive, overarching framework for security policies and guides security teams in identifying possible attack vectors.

Scenario overview: the asset being protected is military targeting data on a covert, hostile headquarters (HQ) building that is scheduled to be targeted with an air attack in the next week. For succinctness, the hostile group will be named the Bad Guys (BG).

Confidentiality:

Low: A low loss will be defined as BG becoming aware that some data is known about this location, but not what that data is.

Medium: A medium loss will be defined as BG becoming aware that Good Guy (GG) forces know that this target is operating as a headquarters location.

High: A High loss will be defined as the same as a medium loss, with the addition that BG becomes aware that a strike is scheduled on this location.

The consequences will entirely depend on how BG reacts to the gathered information. Broadly speaking, if BG relocates their HQ prior to a strike occurring, the damage would be medium or high, depending on how important this particular HQ is. If BG does not relocate, the consequences could be categorized as low.

Integrity:

Low: A low loss will be defined as BG deleting random pieces of information.

Medium: A medium loss will be defined as BG modifying critical data to random values.

High: A high loss will be defined as BG manipulating specific pieces of information to a desired value.

The consequences this time depend on how well GG can recover from the loss. Assuming there is no back up data available to restore the information, recovery could be as simple as referencing the latest printed out version (the teams that perform these functions print a lot of this information out), which would have a low impact. In the worst-case scenario, BG is able to change the target coordinates to a non-combatant location, for example, a nearby school or hospital. Failing to catch this would result in enormous consequences. Another scenario with high damage would be if the corrupted data could not be rectified, as GG forces would need to start from scratch on gathering information about this target, giving BG plenty of time to relocate.

Availability:

Low, medium, and high loss of availability can be defined in terms of how much time the information is unavailable to planners.

This likely has the lowest consequences out of all the pillars, as these systems are built by the lowest bidder, and everyone involved is used to them failing regularly. Recovery for any loss of availability would simply entail referencing the latest printed out data until the data can be accessed again. This is an inconvenience but would likely not have a low impact.

R1 Ricardo:

My own scenario played out very similar to yours, with availability being not as critical of a risk. After reading through your scenario, I started thinking about just how much damage could be done within the confidentiality and integrity domains. You touch on the chaos that could result from the manipulation of data, and the potential of that would probably make for a good comedy sketch. For confidentiality, I was thinking about how some critical data (credit card numbers for instance) could be split off into their own database to reduce the chance of the data being compromised. But even something as simple as a customer name could be a big deal. I’m imagining the newspaper headline after a breach: “Famous politician checked into hotel the same night as famous only fans model”. The potential damage seems large for data breaches of what looks to be fairly inconsequential data.

R2 Brianna:

HFT's are a pretty fascinating example for this discussion, and that we hear surprisingly little about in terms of cyber security breaches. HFT algorithms mostly seem to be about who’s algorithm can process data faster than the competitors, and doesn’t leave time to verify the information coming in. We’ve also seen how devastating errors in this process can be, with simple unintended errors resulting in multiple “flash crashes” which can bankrupt companies in minutes. Though it must be said that one benefit of these precious errors is that HFT’s invest heavily in developing monitoring programs, which work in tandem with the HFT algorithm to prevent it from going off the rails. All in all, HFT’s present a lot of good discussion points for this topic.

R3 Jennifer:

Oh, that's an excellent example, and this is one where I’m legitimately surprised that we don’t hear more about. It seems to me like these systems would be prime targets for various types of attacks. In any school there’s going to be a not insignificant number of complacent teachers and administrators, another group of teachers and administrators whose tech literacy is somewhat lacking. There’s also a high number of motivated students who would love to erase an absence, raise a grade, or just cause some mischief for fun. And finally, these schools are mostly government run, and are famous for having antiquated systems built and maintained by the lowest bidder. So, I’m going to say that the fact that we’re not getting daily stories of students, or angry parents, hacking into some unlucky school’s systems is an absolute win. Throwing out a hypothesis, this may be because by the time schools went digital with their systems, the students were no longer tech native (I believe they’re now best described as “app native”) and no longer have the skills necessary to cause this kind of havoc.

Also, just commenting on a pattern I’ve noticed. My example and all the ones that I’ve replied to, all had the same high confidentiality, high integrity, but low availability scores. It just makes me wonder what sort of system might have the reverse pattern, with low confidentiality, low integrity, but a high availability need.