Systems Investment: The Asset Management Industry's "Grey Rhino" Call for 2023

Years ago, in a different incarnation, I collaborated with a large team to build a Security Risk Assessment for a large software company's customers. While I was just a traffic-cop, ensuring that the cars moved and the lights changed on time, the experts who truly built the SRA took an interesting approach- they helped customers create a "Business Risk Profile" and a "Security Readiness Profile" and suggested that if they didn't match, something had to be done. Put another way, if the business risk was far greater than the security readiness, disaster was on the horizon. Similarly, if the security readiness was far ahead of the business risk, they could slow down investment. We worked with about 200 enterprise customers and found that just about two percent were in the latter situation. About five percent had an approximate match, while a **whopping ninety-three percent had business risk far greater than their security readiness.**

This was twenty years ago. While we've had decades to learn, and while security has gone from a side-subject to the core, I can state without hesitation that, should we modernize the methodology and apply it again, we'd get the same ratios in the end.

If we expand this notion to the area of "Systems Readiness" I believe we'd get a similar picture. Organizations tend to grow ahead of their systems and often invest "after the fact." Not all, mind you, as clearly, the disasters that never happened are for the most part disasters averted by systems, but the frequency of system-meltdowns has actually increased. Recent debacles – like FTX and Southwest Airlines- bring this into bold-relief.

Now, imagine other sectors succumbing to system failures. Imagine, for instance, life-saving industries like healthcare or emergency relief coming to a standstill? Less dramatic but also frightening is the Asset Management industry, which has $120 trillion Assets under Management (AUM) world-wide. System Failure in Asset Management could not only herald "company extinction" events but also industry-morphing disasters. Anyone who worked through the GFC in 2008-2009 understands what can happen. Suddenly.

But not without warning. And there's the rub.

Early, distant warnings are a key reason to invest in the right systems. Mature data platforms can help an organization manage risk in ways both small and big. Resilient security and monitoring can stave off attacks and keep systems healthy and running. With Asset Management specifically, the importance cannot be overstated. The "payload" of disaster is measured in numbers higher than global GDP.

Great systems allow for several things at once-

1. The smooth and efficient management of the business- in peacetime.
2. The management and minimization of risk- in peacetime.
3. Quick reaction and protection- in wartime.
4. Massive loss prevention- in wartime.

"Peacetime" operations are important. That is the core business. But "Wartime" management and mitigations make it possible for the organization to live a long-life.

For Asset Management, great crossover systems must include state-of-the art data management, an AI-chassis for predictive decision making, world-class security, cloud-native vendor protections, and a clear and actionable analytics module that puts the rest in a "usable" mode.

Even the best among organizations suffer when they get complacent about systems. Black Swans do happen but they are not possible to predict, by definition. But the "Grey Rhino" event- the disaster that we had enough information to avert-can happen on our watch if we don't invest in the right systems and embed them in a culture of systematic learning.