Black Swan Risks[1]

Bob Prieto

Much has been written on Black Swan type risks, sometimes treated as the risks from Unknown Unknowns. Do Black Swans inhabit the world of program management and are they truly Unknown Unknowns?

In 17th century Europe all observable swans were white and by extension all swans were therefore assumed to be white. No non-white swan had ever been observed.

In the 18th century, however, black swans were discovered in Western Australia and that discovery undermined the statistics of swans to that date. Previously, the "risk" of a Black Swan was essentially nil but upon recognition that the improbable was not the same as the impossible the possibility of Black Swans became more likely.

What had changed that made Black Swans more probable? Simply put our perceptions were broadened. In this article we will look at large programs, what creates the possibility of Black Swans and what are some of the new risks we must pay attention to.

[1] *Second Editions are previously published papers that have continued relevance in today's project management world, or which were originally published in conference proceedings or in a language other than English. Original publication acknowledged; authors retain copyright. This paper was originally published in the January 2011 edition of PM World Today. It is republished here with permission of the author.*

Possibility of Black Swans

Program Management is very much about meeting the challenges of scale and complexity. These challenges largely focus on the management of known knowns and known unknowns.

But large programs by their very nature move into a new neighborhood where previously rare unknown unknowns are more prevalent. In effect, large program risks grow in new non-linear ways. What causes this growth?

Simply put:

- Scale and complexity move you into a new neighborhood where black swans may be more common
- Scaling drives non-linear and non-correlated growth in risks
- Complexity masks existing risks
- Complexity creates new risks

So what are Black Swans?

First they are outliers, beyond the set of expectations we have about allowable "value." They are outliers since we ***believe*** we have no past experience to suggest the possibility. I emphasize the word "believe" here since I will later suggest that there is a reasonable expectation that large programs are "neighborhoods" that Black Swans visit.

Second, Black Swans have a significant impact not only on the program but on the psychology and behavior of those implementing the program. They often cause a new paradigm to develop that may not fundamentally reduce risks.

Third, we rationalize after the fact that it was in effect predictable. While in some instances this may be true, often it defies rationality and thus a focus on resisting, responding and recovering from these unknown unknowns through resiliency is a more appropriate focus.

In Michael Lewis's book, *The Big Short*, there is an illustration of a business model that masked what otherwise should have been a reasonable expectation. He describes some of the models used by ratings agencies to rate mortgage-backed securities, reporting that at least one agency used a model for home price increases that could not accept negative numbers.

As an engineering and construction example, many estimating and business modeling programs provide for inflation of costs over time and even model the variance of such costs over time. Do they allow for deflation?

In my view the main point is to build resilience against outlier risks that can occur and capitalize on outlier opportunities. This concept of building resiliency into the program structure and strategies is an important one.

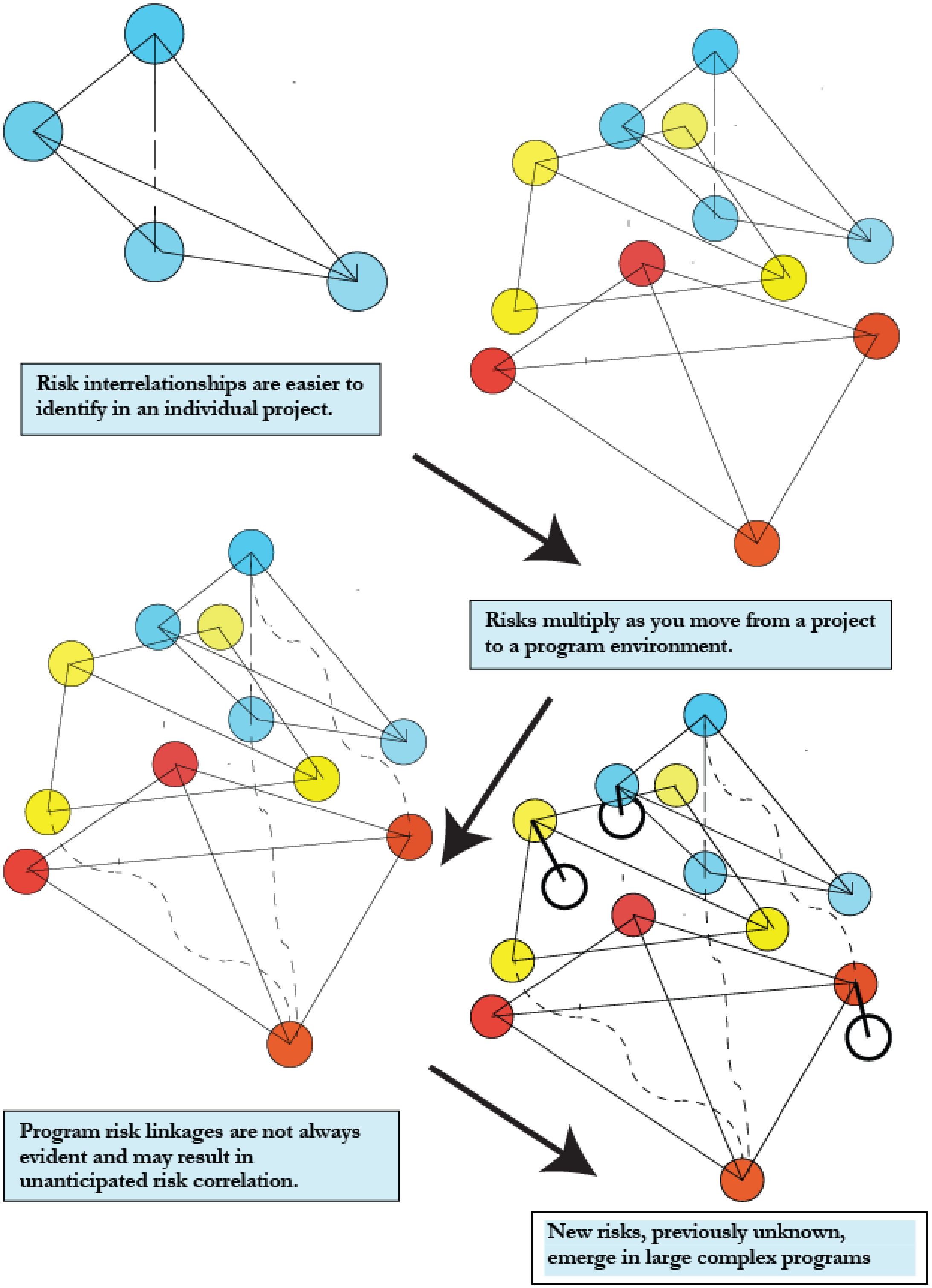
New Risks in Large Programs

Complexity and scale create an attractive environment for Black Swans. They create a hidden, interlocking fragility while at the same time giving a perception of stability in this complex system.

Vulnerabilities enter large programs, project organizations and other human-designed systems as they grow more complex. Increasingly these systems and their myriad of relationships, including hidden relationships, are so complex that they defy a thorough understanding

As complexity grows insufficient attention is often paid to the introduction and proliferation of new links with new risks. As a result, many programs continually implement workarounds and "fixes", which ultimately add to the total life cycle cost and often sow the seeds of new risks and new failures.

(see chart below - next page)



Risk interrelationships are easier to identify in an individual project.

Risks multiply as you move from a project to a program environment.

Program risk linkages are not always evident and may result in unanticipated risk correlation.

New risks, previously unknown, emerge in large complex programs

To exacerbate matters, the possibility of random failure rises as the number of combinations of things that can impact the program grows. This is the non-linear effect previously described. The enormous complexity of large programs means that even tiny risks and attendant failures can cascade to catastrophic proportions.

Severe impacts from Black Swans are almost guaranteed to occur in some complex programs, especially those with strong externalities or of a long duration. The statistics of events in manmade systems is starting to resemble that of natural phenomena like earthquakes, they are bound to happen.

In March 2000, a fire struck an Ericsson semiconductor plant in New Mexico choking off the supply of millions of chips they were counting on to launch a new mobile phone product. As a result, Ericsson was ultimately driven from the market to its competitor's advantage. They had failed to recognize the plant as a chokepoint in a complex global supply chain.

The inherent weaknesses of a complex system reveal themselves in the face of turbulence or stress.

As the complexity of systems increases, the exposure to Black Swan risks grows. But these risks do not need to be unmitigated.

In each Black Swan event we have seen certain core lessons learned which must be acted upon by the Program Manager. These lessons include:

- Recognition that "core capacity" of complex programs and systems is essential.
    - Adequate capability to meet routine needs contributes to the program's ability to respond to Black Swan events. But it is not just "more" capability, but also the degree of interconnectivity of the various elements of the system, its flexibility and redundancy. Or in other words its resiliency,

sensitive to the fact that this interconnectivity may also create new vulnerabilities.

- Understanding the link between process and non process infrastructure

- Recognizing the real cost and real risk that come from failing to keep the program performance and capability at high level

    - I often wonder how program performance would improve if as much attention was focused on program organizational performance as often is focused on the approval of the addition of the next staff member!

Resiliency is built on a comprehensive understanding of the required level of performance that an organization requires to meet both normal as well as off normal events. Assessment of organizational resiliency must be risk based. For resiliency management to be effective and support organizational resiliency, an organization should at all levels comply with the following principles:

- Risk management creates and protects value and promotes resiliency as one of the strategic business objectives of an organization.
- Risk management, including a specific assessment and management of risks that affect the resiliency of an organization, is an integral part of all organizational processes.
- Resiliency management is not a stand-alone activity that is separate from the main activities and processes of the organization.
- Resiliency management, like risk management in general, is part of decision making. It helps organizations make informed choices, prioritize actions and distinguish among alternative courses of action.
- Resiliency management explicitly addresses uncertainty in terms of initiating events; organizational and systemic response; and nature and timing of recovery.
- Resiliency management is systematic, structured and timely. It encompasses all aspects of an organization and the full life cycle of all organizational activities.
- Resiliency management is based on the best available information. Inputs are based on a broad set of information sources and include expert judgment. It should take into account, any limitations of the data or modeling used or the possibility of divergence among experts.
- Resiliency management is tailored to the organization's external and internal context and risk profile.
- Resiliency management takes human and cultural factors into account to the extent that they can facilitate or hinder achievement of the organization's objectives.
- Resiliency management is transparent and inclusive and includes involvement of stakeholders and decision makers at all levels of the organization.

- Resiliency management is dynamic, iterative and responsive to change. As external and internal events occur, context and knowledge change, monitoring and review take place, new risks emerge, some change, and others disappear. Therefore, resiliency management continually senses and responds to change.
- Resiliency management facilitates continual improvement of the organization.

We need to be **SMART** about the types of Black Swan risks that large programs may face:

- **S**ystem Risks
- **M**aintenance & Operation Risks
- **A**ttitude Vulnerabilities
- **R**isk-taking Vulnerabilities
- **T**ransitional Risks

System Risks

Prior Black swan events require us to take a "systems perspective" when assessing and managing risks in large, complex programs. Not surprisingly, the first set of risks we need to be **SMART** about deal directly with the very nature of the system.

In particular, we need to understand the risks associated with:

1. Failure to recognize the program as a growing and ever more complex system
   This is perhaps the most fundamental risk we have. Projects, processes and people comprising a large program do not exist in isolation.

2. Inadequate "system" understanding
   It may not be "rocket science"…or a high-technology defense system…but it is no less important to understand what may go wrong, and how to detect and remedy it.

3. Positive feedback loop risks
   Also described as "progressive" failures.

> Deepwater Horizon
>
> A series of calculated risks, each a reasonable risk, combined to create an event well beyond the consequences of each risk taken.

4. Centralized control weaknesses in complex systems
   There is a need for "interoperability" and an ability to "see" the situation. Partial decentralization of systems is required.

5. "Tight Coupling" of systems
   Simply put an event in one system or project leads to an event in another in short order.

Deepwater Horizon

Workers had difficulty monitoring key data during a critical time in the final hour before the Gulf of Mexico oil rig explosion because so many activities were happening at once.

Data presented by a support services coordinator to a federal panel investigating the April 20 disaster shows there was a sharp rise in pressure that was later followed by a sharp drop in pressure

But workers on the rig later said that there were so many simultaneous activities, starting with the displacing of mud to the pumping of fluids overboard, that it was difficult to see what was going on.

Photo courtesy of U.S. Coast Guard.

6. Failing to **KISS**
   "**K**eeping **I**t **S**imple…**S**tupid." We must recognize some classes of systems and certain organizational and project approaches are inherently open to chains of failure. In such systems, adding additional safety or control systems only raises the level of complexity.

7. Inadequate "core capacity"
   The importance of interconnectivity, flexibility and redundancy to system responsiveness to unplanned events.

   All too often we emphasize "reach" over "responsiveness" when making key decisions regarding program and organizational investments.

Consideration of these risks will enhance the resiliency of large, complex programs.

Maintenance & Operation Risks

If "system" risks focus on ensuring that the right system is put in place, then "maintenance" risks are focused on keeping it that way.

Specific risks include:

1. Failing to recognize the importance of "state of good repair"
   Programs and program teams in a "state of good repair" will respond better to Black Swan risks.

   There is a tendency to compensate for existing maintenance and operational vulnerabilities by adding on top of the existing base system. In complex systems, in particular, this can act to create new risks. The "foundation" must be strong.

2. Inadequate renewal of contingency planning
   The management systems and frameworks our programs are built on are not static, nor are the risks they face. Contingency planning must be undertaken recognizing the dynamic environment within which our program environment exists as well as its own inherently dynamic nature.

3. Inadequate operating provisions to limit disturbances
   Failure must be contained or "localized" to prohibit "tight coupling" effects from taking hold.

Attitude Vulnerabilities

In contrast with system and maintenance risk that focus on whether the right management systems and frameworks are in place and whether they are sustained properly, attitude vulnerabilities address our willingness to accept an unexpected or undesired "truth." Specific "attitude" risks include:

1. Cognitive lock
   In life, particularly when we are under stress, we expect certain situations to evolve in certain ways. Sometimes they don't. Cognitive lock occurs when we hold onto a course of action against all contradictory evidence. This can be particularly disastrous when combined with a complex system such as those represented by large programs and often requires a fresh pair of eyes to see the new "truth" in front of us. I include haste as an attitude vulnerability given the risks often incurred, unknowingly, when blindly charging ahead. As issues arise, where was the fresh pair of eyes or the process to take a fresh look?

2. Over-commitment to bureaucratic goals
   The goal has been set and any deviation from the goal is not acceptable. Problems that arise are ignored if they put the goal at risk. Does mere achievement of the bureaucratic goal ensure we have accomplished our strategic business objectives?

   We confuse outputs (project management thinking) with outcomes (program management thinking).

3. Prisoner to Heuristics
   Past experience or what we've heard prevents us from taking a broader look. We adopt a perspective of "it never happened, so it's not credible."

   Being a prisoner to heuristics also involves a failure to consider what we see or learn from analogous systems or settings.

4. Denial
   Conventional risk and threat analysis has us consider a range of "likely" scenarios and design our systems to resist, respond and recover from such scenarios. But the "unlikely" is also possible and it, too, must be considered. How do you address these "unlikely" scenarios in program design and operation? At one level you can't because one can always postulate another "unlikely" scenario that will defeat any specific measures you undertake. So what is one to do?

In many ways this brings us full circle to the need to have inherently flexible, redundant and reliable systems. "Core capacity" provides the trained program manager with the tools to address a broad range of "unlikely" scenarios.

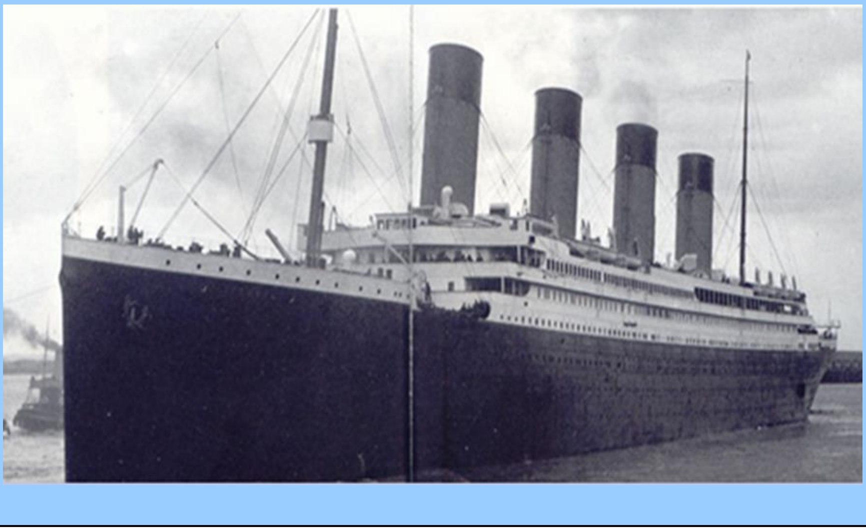
Contingency planning must include training in the capabilities and limits of various tools at the program team's disposal. The "unlikely" must be part of our planning processes.

Titanic - April 14, 1912

- Sea dotted with hundreds of ice flows…no extra lookouts posted
- Captain received 6 warnings of ice field from ships in area
- No binoculars available in crow's nest …early warning nearly impossible
- Very hazy conditions…lookouts confused in what they saw ahead of them
- Titanic sped toward ice field at 22.5 knots (10 knots recommended for conditions)

Motivations for speed

- Desire to break transatlantic speed record
- Encouraged by project sponsor who was on board for maiden voyage



5. Failure to learn "lessons learned"
   We have seen many of these lessons learned in prior programs subject to events of scale.

Risk-taking Vulnerabilities

None of us likes to be wrong. But the way we perceive risks and handle mistakes affects the range of actions we are willing to consider when faced with extreme situations. Risk aversion replaces risk management. Two particular risk-taking vulnerabilities are worth calling out.

1. Litigation constrains risk-taking in the early phases after an event of scale
   There is reluctance to recognize the risk or changed circumstance for fear of increasing our liability. Finger pointing may replace a helping hand.

2. Fear of "satisficing"
   We are often called to make decisions or take actions in the absence of complete information. Our willingness to take action and move forward with an apparently workable solution is often a function of how mistakes are perceived and handled.

9/11 Response

Running heavy cranes out across the "debris field" following the collapse of the World Trade Center was an example of willingness to "satisfice." No as-builts existed and a high degree of judgment and risk-taking was required. How might we have handled a mistake that sent a crane toppling or crashing through the sub-basement structure?

Transitional Risks

"Change" is the watchword of life. But in the process we must recognize that complex programs and their management systems, and, for that matter, systems in general, are often most vulnerable immediately before, during and immediately after this change process. What are some of these transitional vulnerabilities and what must we be cognizant of as we move through these transition stages?

They include:

1. Inadequate use of currently deployed resources
   There is a tendency to look for the "silver bullet" as opposed to better deploying and applying the resources at hand.

2. Change processes further stress existing systems
   Change for change's sake is not necessarily the answer and, approached narrowly, may increase the overall risks we face.

3. New system failure rates not planned
   True operating characteristics and failure rates of new systems can only be understood after an extended period of operating under both good and bad conditions. The old adage that you "don't know what you don't know" is particularly relevant during a transitional period.

4. Technology put ahead of people
   People cannot, nor should not, be taken out of the loop. Technology is a powerful enabler of people…but it needs to fit them, not the other way around.

Today's program manager must explicitly test the program design, processes, procedures and organization against these SMART risks and vulnerabilities to ensure a resilient strategy and program execution framework.

Some Final Thoughts

Taleb describes Black Swans as an event with the following three attributes.

"First, it is an *outlier*, as it lies outside the realm of **regular** (*emphasis added*) expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme impact. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence *after* the fact, making it explainable and predictable."

So in hindsight, one can always argue that a Black Swan was a **knowable** unknown and this is the case most certainly with September 11th which Taleb uses as an example of a Black Swan event and an attack which many have classified as knowable given prior attempts to bring the buildings down and prior use of suicide planes.

Most importantly, I think it is important to consider Taleb's first point, namely an outlier outside the realm of **regular** expectations. In the example in this paper, the factory fire may have been a reasonable event to be considered but in complex global supply chains a singular fire at a component level supplier would not be one generally anticipated to eliminate a firm from a major market. At that time it was an outlier, outside the realm of **regular** expectations.

Increasingly large programs introduce levels of complexity that provide convenient territory for Black Swans to nest and breed. They lie outside the realm of **regular** expectations. The point, often made, on turning as many knowable unknowns into known unknowns is one I could not agree more with and one which I believe is aided by a program management approach that focuses on the "white space" between projects in order to ensure an "outcome" versus a project approach, which takes a more limited scan of the external environment and its impacts on the project's ability to produce certain "outputs". In a program context, good risk management is about limiting the neighborhoods where Black Swans can be by more rigorously examining these potential nesting and breeding grounds (knowing more) and most importantly building in resiliency.

Black Swans should not be used as an excuse for ineffective risk management.

About the Author

Bob Prieto

Senior Vice President
Fluor
Princeton, NJ, USA

Bob Prieto is a senior vice president of Fluor, one of the largest, publicly traded engineering and construction companies in the world. He focuses on the development and delivery of large, complex projects worldwide. Bob consults with owners of large capital construction programs across all market sectors in the development of programmatic delivery strategies encompassing planning, engineering, procurement, construction and financing. He is author of "*Strategic Program Management", "The Giga Factor: Program Management in the Engineering and Construction Industry" , "Application of Life Cycle Analysis in the Capital Assets Industry"* and *"Capital Efficiency: Pull All the Levers*" published by the Construction Management Association of America (CMAA) and "*Topics in Strategic Program Management*" as well as over 500 papers and presentations.

Bob is a member of the ASCE Industry Leaders Council, National Academy of Construction, Fellow of the Construction Management Association of America, member of the World Economic Forum Global Agenda Council, and sits on several university departmental and campus advisory boards. Bob served until 2006 as a U.S. presidential appointees to the Asia Pacific Economic Cooperation (APEC) Business Advisory Council (ABAC), working with U.S. and Asia-Pacific business leaders to shape the framework for trade and economic growth and had previously served as both as Chairman of the Engineering and Construction Governors of the World Economic Forum and co-chair of the infrastructure task force formed after September 11th by the New York City Chamber of Commerce. Previously, he served as Chairman at Parsons Brinckerhoff (PB). Bob can be contacted at Bob.Prieto@fluor.com.