Rethink Risk Through The Lens of Antifragility

Bill Murray
Dave Aron

April 2017
Summary

This Position Paper argues that the way we think about risk isn’t serving businesses and government organizations well enough in the 21st century, and that a new mindset, namely that of antifragility, is a promising augmentation:

• Enterprise Risk Management alone does not fully protect us, nor does it help us to take intelligent, value-creating risks in a world of increasing volatility and uncertainty where the impact of shocks is more widespread and costly than a decade ago.

• In their quest for growth and efficiency, leaders are engineering fragility into their businesses, often accidentally.

• Antifragility is a different perspective, focused on ‘bending luck’ by creating options, so that we win more than we lose when shocks, stressors and risks hit us.

• Antifragility fuses value creation with risk management in highly volatile and uncertain environments.

• Antifragile practices can be applied at component, process and business model levels, touching all aspects of our businesses, and should be embedded in business strategy, IT strategy and all other functional strategies.

• IT organizations are pioneering practices that increase antifragility, such as DevOps, microservices and exploitation of public cloud services.

• Antifragility is such a powerful and important quality that enterprises should consider making it one of their dominant success criteria.

In a hyper-connected, highly uncertain world, risk management is failing us

We live in risky times – or more specifically, times of increasing volatility and uncertainty. In the last decade, we have seen the 2008 credit crunch, the 2010 Deepwater Horizon oil spill, and the Arab Spring in 2011-12. In 2016, we experienced the vote for Brexit, the election of President Trump and the start of a populist movement that could bring trade wars, geopolitical conflicts and civil disorder. We are also seeing more and more ingenious and prevalent cyber attacks on corporate, national and international infrastructures.

The volatility and impact of all these risks are massively amplified because we live in a hyper-connected world where everything – from nuclear power plants, factories, vehicles, fridges and hospital equipment to wearable and invasive devices – is increasingly hyper-connected, inspectable and controllable. Businesses can be remarkably adaptive, but it does not help that we often design fragility into our systems and processes, particularly through efficiency and cost-cutting initiatives.

Are we ready for such heady and unpredictable levels of risk?

We at Leading Edge Forum contend that our businesses and government agencies have sleepwalked into the 21st century with organizations that are not fit for purpose. We need to evolve many aspects of our organizations, including how we think about, sense, manage, monitor and more generally address risk. We argue that the traditional approach to risk management in business has several significant flaws.

First, there is the sense that with risk management we are, to some extent, managing risks that we have already seen or can already imagine – that could be labelled ‘known unknowns’. This could be cruelly labelled as ‘managing risk through the rear-view mirror’, and does not address unexpected risks. (You may well ask how it is possible to manage those, and you will see our response later in this document.)

Specifically, the current approach to risk management fools us that we have risk under control, because we understand and have mitigation plans for expected risks. However, as author
Nassim Nicholas Taleb points out, many historical events have been caused by ‘black swans’: large, unexpected risks (which we later post-rationalize as if they were expected). The Fukushima nuclear incident was a negative black swan; Google’s creation of Gmail arguably a positive black swan.

Another issue is that many aspects of risk management continue to require human intervention, which is sometimes impractical in a hyper-connected, high-speed world. Just for example, in 2016 we saw successful military tests of self-organizing, self-managing drone swarms. Many of the processes and policies for launching a single military aircraft require human intervention and paperwork, with lots of lags in the system; launching and re-launching drones and drone swarms will demand higher speeds and less human intervention. Similarly, in a fast-moving, hyper-connected world, the implementation of much risk management will need to be automated, based on machine intelligence.

But the most troublesome aspect of risk management is its separation from value creation and growth. Although security and risk managers are keen to talk about the value of risk management, that is not the issue we are raising. The issue is that the places and mechanisms that we use to discuss and decide on risk management are not the same as the places and mechanisms that we use to discuss business value and business growth; they are separate domains.

We may label this way of thinking as an ‘engineering’ view of risk: all risk is bad and must be eliminated, and risk has nothing to do with value creation.
This view of risk leads to several problems, including:

- Wrapping companies up in legislation that is largely built around risks that have already happened, often giving a false sense of security that because they have ‘ticked all the boxes’ they are safe. (There are several studies observing this effect – e.g. after Sarbanes-Oxley was introduced.)

- Missing the considerable upside of taking intelligent risks.

- Living with unresolvable tensions between feeling the need to address every potential risk, yet having limited budget for risk management, and the imperative to make a profit and be agile.

Despite these tensions, our way of thinking of and dealing with risk in companies is deeply ingrained, but must be changed if we are to survive and thrive in the 21st century.

**Antifragility is an exciting alternative that fuses value and risk, and CIOs and IT executives are well positioned to help**

If instead of the ‘engineering’ view of risk, we think of risk as an inherent, and not always bad, feature of all business, all processes and all value flows, then we approach what we might label a ‘financial’ view of risk. In this view, companies choose activities that have attractive risk/return profiles or ‘yield curves’, and try to bend those yield curves to be even more attractive.

---

21st Century Organizations fuse value and risk in their decision making
A powerful way to approach this view of risk is the relatively newly named concept of antifragility. Coined by Nassim Nicholas Taleb, who himself comes from a financial trading background, antifragility refers to a property of any thing or system (company, country, business, species, etc.) that causes it to gain from shocks, stressors and risks\(^v\). Antifragility in business is real: Toyota has been hit by shocks and recovered to be stronger. The firm was severely damaged in 2009 and 2010 with the largest car recall in history followed by a massive tsunami that wreaked damage in its international supply chains. Yet Toyota’s fiscal 2013 profits were more than four times its 2010 earnings, and three times 2012’s. The company has arguably reclaimed its place as the world’s most successful car maker.

Another great example of antifragility was shown to us by data privacy startup Integris Software\(^1\) during our April 2017 Silicon Valley and Seattle study tour. Integris provides services that help companies comply with increasingly stringent data protection regulation, notably the European Union’s GDPR regulatory framework. The stringency of its requirements, severity of penalties up to 4 percent of global group revenues) and timing (need to comply by 25 May 2018) represent a considerable shock to many companies. Integris’s software helps companies more easily understand what data they have. We were told of Integris clients getting stronger through the use of such services, and being able to use their data more effectively to create business value with customers. Another GDPR startup, Trust-hub\(^2\), told us a similar story.

We tend to think of being robust or resilient as the opposite of being fragile, but in fact, they are just waystations en route to the true opposite of fragility: *antifragility*. The figure below shows the response of systems when risks/shocks/stressors occur. A fragile system quickly deteriorates – like a paper house in a storm. A robust system holds out longer – like a brick house in a storm – but ultimately breaks too. A resilient system bends but doesn’t break, and ultimately comes back to normal – like a supple tree in a storm. An antifragile system adjusts and ultimately comes back stronger, like the human race after an epidemic. LEF’s Lewis Richards is researching how to strengthen antifragility in the 21st Century Human; we can become stronger as we seek out things that stress our abilities.

---

2. https://trust-hub.com/
Becoming antifragile is not about increasing robustness or resilience in the face of expected shocks. It is about systematically stressing the organization, and learning and restructuring to take advantage of unexpected shocks.

The goal of antifragility is to ‘bend luck’. An antifragile approach tries to bend the downside risk portion of the yield curve upwards, through what we might call ‘robustification’, and amplify the positive outcomes of the upside of the yield curve. In other words, we try to create an organization that stands to gain more in the good times than it stands to lose in the bad times; a ‘positive asymmetric position’. If we can do that consistently, we will get stronger and more successful over time.

Bending the downside up, ‘robustifying’, consists of some familiar risk management disciplines but also some counterintuitive ones, such as creating redundancy, adding extra layers, and deliberately damaging then repairing systems and processes.

Amplifying the positive outcomes of risk, bending the upside up, is less familiar territory. It consists of creating options and aggressive experimentation. As those familiar with financial derivatives will know, a financial option is the right, but not the obligation, to buy or sell something at a given price in the future. For example, you may buy an option that conveys the right to sell 1,000 Microsoft shares at $75 on 1 January 2018, but not the obligation to do so – i.e. if Microsoft’s shares cost more than $75 on that date, it is better to sell at the market price, so it is better not to ‘exercise’ the option.

We may similarly create business conditions that convey the right, but not the obligation, to perform specific business activities, if the conditions warrant it. Cloud computing contracts may be thought of as consisting of – or at least including – options: you have the right to scale up (and down) your infrastructure, software or other service needs, at a pre-agreed price, if demand warrants it. Traditional in-house infrastructure affords no such rights, or at least they tend to be slow and/or expensive. Other methods of creating business options include having alternative suppliers and systems; creating teams with multidisciplinary, versatile members; building options into procurement contracts; and securing guaranteed access to scarce resources, including talent.
This very attractive state, of having bent luck through ‘robustifying’ the downside and amplifying the upside with options, may be termed *convexity*. Making an organization antifragile means maximizing the convexity of the yield curves in the organization – for example, those related to the supply chain, procurement, finance, product development, IT services, projects, talent acquisition and, of course, enterprise risk management itself.

Antifragility is a valuable state but one that is hard to achieve in the business world. Even if a company can’t achieve full antifragility, LEF believes it is also helpful to consider the concept of relative antifragility: being more antifragile than your competitors. If you can withstand/learn/grow from shocks better than your competitors, then even if you take a bit of a hit, you are likely to increase market share and all other good things (revenue, profit, etc.) in the medium to long term.

**Antifragility happens at three levels in a business**

LEF believes that we can inculcate a business or government agency with antifragility at three levels.

![The three levels of a business where antifragility can be applied](image)

First, the individual assets/components can be made antifragile. A good example here is making our talent pool antifragile by learning to use talent marketplaces such as Topcoder, 99designs and InnoCentive. Whilst they may not be applicable for all our human resources, getting away from dependence on a relatively small pool of internal employees that is hard to grow and may contain specific single points of failure, and exploiting large pools of talent ready to work at the drop of a hat, is very powerful. The Infrastructure-as-a-Service and Software-as-a-Service public cloud layers of the Matrix, as well as more sophisticated services (like Machine-Intelligence-as-a-Service) also sit here, providing components that can flex in terms of scale to exploit volatility in demand automatically, at pre-agreed prices. Utilizing the Matrix is the key to building and sustaining the kind of ‘plug and play’ business models used by the digerati.

Second, the business processes of a business can be made antifragile, so that they can adapt positively in the case of stressors and shocks. One technique that helps here is employing internal ‘masters of disaster’ or ‘chaos monkeys’ to continually challenge processes so that they learn to heal and, crucially, improve*. Business-Process-as-a-Service capabilities within the Matrix also contribute here.

At the top level, creating and/or migrating to business models that are more antifragile (i.e. less susceptible to negative shocks and able to gain from positive shocks) is the key. It is often said that during a gold rush, the guys who are sure to make money are those selling shovels. Updating that concept a couple of hundred years, and generalizing it, we can see that platform business models can be antifragile. To put it overly simply, iTunes’ business doesn’t stand or fall on an individual artist’s music being popular. More generally, both the orchestrator and key providers in a platform business ecosystem can gain from volatility in the market*. 

---

*These terms are used for illustrative purposes and do not reflect actual terminology.
We can use a martial arts metaphor to understand this three-layer model of antifragility. If someone is going to punch you (the risk/stressor/shock), strengthening your body so it can take the hit is like the bottom layer (antifragile components). Learning techniques and sequences to defend yourself against the blow, and maybe turn it to your advantage, is like the middle layer (antifragile systems/processes). Sensing danger coming, and hence not being there when the blow comes, is the highest and most effective form of antifragility; this is akin to business model antifragility.

We should strive for antifragility in all three layers, but as in the martial arts metaphor, business model antifragility is perhaps the most powerful.

Antifragility is such an important quality that it should be one of the most important features of a successful enterprise. If we are antifragile in an increasingly volatile environment, value eventually comes – through revenue, profit and growth. Traditionally, risk management metrics would be subservient to the revenue and profit growth figures. But if we have a business that makes sense, keeping it antifragile (i.e. benefiting more from upside shocks than losing from downside shocks) at the business model, systems/processes and component levels, means more value will come.

Nine stratagems for increasing antifragility

We have established that it would be very desirable to make our businesses antifragile in the face of high levels of volatility and uncertainty. But how do we do that? Here are nine tactics to increase antifragility, rolled up into four high-level stratagies. There are organizations that are doing some of these already (though perhaps poorly); some are new to most; and some are in tension with what we are doing already.

1. Adapt continually through experimentation. One of the foundations of antifragility is the ability to sense and adapt to change.

   a. Sense and learn. Perhaps the most obvious of the mechanisms for being more antifragile is to become better at sensing and learning. If we can see what’s coming, that allows us to adapt and orient to better exploit it. This includes sensing and learning about all aspects of our environments, including technology, societal, risk, regulatory and competitive trends and disruptions. Applying better and more business intelligence is a powerful component and business-systems-level lever here. Creating sensing capabilities in the ecosystem is a powerful extension of this beyond company boundaries. A great example of this is banks sharing fraud data early and often – it makes their business systems much more antifragile. Internal startup-like experiments in-house and/or very tight linkages to innovation incubators/accelerators/catapults create sensing and learning at the business model level. At the time of writing, this is a very popular strategy for banks, especially around the area of blockchain.

   b. Aggressively tinker. As described in our ‘winning in the 21st century’ model, organizations that hope to win in a volatile world must continually experiment. At the component level, this often takes the form of releasing products early, to experiment and improve. DevOps captures this in its ‘third way’. At a business system/process level, this looks like getting off the strategy-planning-execution bandwagon, selectively performing some ‘unstrategy’ (experiments that are not aligned with strategic direction), and indeed digital business model hacking – trying to work out how to cannibalize/kill your own business. At a business model level, this can mean implementing a lean, startup-type model, building the willingness to ‘pivot’ the business model. Intriguingly, some aggressive tinkering may be automated, using machine intelligence. For many years, some industries that have a high volume of customers have used an approach to pricing that continually experiments with building a real-time price elasticity curve by (for example) charging 90 percent of customers the existing price, 5 percent of customers prices that are 1 percent higher, and 5 percent of customers prices 1 percent lower. They can then use this information to choose to move up or down in price, to maximize profit. Extending this notion of dynamic pricing to product/service features, business processes and all other aspects of the business system makes for an exciting possibility: automated tinkering, learning and adapting.

   c. Adopt a barbell investment strategy. Inspired by the shape of the barbell, this strategy involves investing significantly in robustifying low-risk activities (think existing operations) and in a portfolio of high-risk activities (think digital experiments), but starving the middle of
investment. Each of the high-risk activities should be treated as an option – a right to invest further if the experiment proves interesting. This is different to what most companies do, but can be an optimal strategy when faced with high levels of volatility and uncertainty. The adoption of a ‘pioneer-settler-town planner’-type organization (where pioneers conduct the high-risk experiments, settlers industrialize the successful ones, and town planners operate and nurture the resulting activities) is a powerful complement to a barbell investment strategy.

2. Create a distributed, modular business that is not a single big bet with a huge win/huge lose payoff strategy. This is often in tension with a desire to create efficiency/cut cost through centralization.

a. Distribution. Distributed organizations can learn better from randomness because adverse impacts are isolated. At a component level, this means building business infrastructure (including digital infrastructure) that supports a decentralized model as much as possible. At a business systems/process level, this means creating an architecture that allows diversity of systems and services to be procured and/or created, without causing chaos. An example would be a multi-cloud strategy which helps architect to avoid failure. At a business model level, this means allowing relatively autonomous business units to operate alongside each other. A great example of this is FAVI, a French pressure die-casting company that has evolved to become a group of mini-factories. LEF has suggested it is useful to think of our businesses not as one giant army, but more as a swarm of intelligent drones. The benefits of scale can be combined with more distributed models through information integration, centres of excellence, matrix organization and inter-disciplinary working.

b. Diversity. Diversity in the workplace is a natural accelerator of antifragility, largely because it reduces groupthink and strategic blindspots. At the component level, diversity in management and individual teams, including the use of non-executive members of boards, creates a measure of antifragility. Embedded diversity in the culture is a more substantial, business systems antifragility play. A business model that includes diversity in the investment portfolio, including investment in startups as well as more conventional internal projects, ideally within the broad shape of a barbell strategy, takes antifragility to another level. A key aspect of business model diversity is learning how to work in large-small partnerships (sometimes called ‘David-Goliath’ partnerships) which is notoriously hard but incredibly powerful.

c. Redundancy. Architecting business processes to have some redundancy (as opposed to optimal efficiency) enables quick reaction when circumstances change. In the highly competitive, oligopolistic world of Japanese convenience stores, 7-Eleven Japan has been very successful over the years by on the one hand building a great sense-and-learn capability, with the capability to dynamically test hypotheses, and on the other hand building an agile, multi-tiered distribution system, rather than a hyper-efficient logistics system. This approach has allowed it to adapt better to local circumstances for each store.

3. Learn and adapt through trading. A third foundation stone of antifragility is exposing ideas to the invisible hand of trading, which creates a kind of automated sense-and-adapt mechanism.

a. Trade/create markets. If we can find ways of exposing our components, business processes and business models more to the invisible hand of markets, we are in effect building in antifragility. At a component level, this includes talent marketplaces (such as the Topcoder prize-driven software-development platform) and cloud marketplaces (such as the Amazon, Microsoft, Google and AliCloud ecosystems). At a business process/system level, this means migrating from linear value chains to more loosely coupled ecosystems, and testing products using Agile or Minimum Viable Product strategies. And at a business model level, this means looking to become a producer, provider or owner of a platform business model. Multi-billion-dollar peer-to-peer creative marketplace Etsy is a great example of this, since Etsy and its community are continually experimenting with new services and commercial models: learning, adapting and evolving.

b. Create internal markets. Applying the principle of trading internally also creates antifragility, enabling us to continually learn and adapt depending on our resources and their capabilities. This includes allowing people to choose their projects, rather than managers mandating projects. Companies including Huawei have been experimenting with this bold resource allocation practice. This area also includes the more prosaic topic of collaboration, making it easier to discuss, vote on, decide and adapt ideas with larger, more diverse groups. This
approach should create antifragility through improved sensing and learning, better and faster innovation, and fewer biases and blindspots. At a component level, this requires providing better collaboration tools, and culture, metrics and rewards that are aligned with collaboration. At a business systems/process level, the opportunity is to make more of the work about inter-disciplinary and cross-divisional self-managed teams that are not tethered to the organization structure.

4. Bring the dark side inside. How can we learn even faster than by exposing all our components, systems and business models to market forces? The answer is by deliberately introducing shocks and negative stressors into our businesses. In a sense this is almost the opposite of the aggressive tinkering stratagem above. This is tinkering to damage our business, to make it ultimately stronger. Just as species including humans get stronger after an epidemic, businesses that survive attacks get stronger too. Adversarial techniques in artificial intelligence are a good example of this stratagem. About a decade ago, one UK charity’s CIO told us that he felt that his risk management messages weren’t getting through, so he went into the office one weekend, unplugged a server, and took it home. When he arrived at work on Monday morning, there was much consternation, which ultimately resulted in more redundancy and better risk management. This has been formalized recently with some of the digerati employing ‘masters of disaster’ – people paid to try to break the business – typically at a component level. There are also pieces of software like Chaos Monkey, which randomly terminates services to check how the system could cope. LEF has written about extending this concept to business strategy by employing teams to try to develop business models that would destroy the company.

There is strong digital connection to all nine stratagems

Becoming antifragile is an intelligent response to high levels of volatility and uncertainty. It is a concept and mindset to be included in an organization’s business strategy, IT strategy and enterprise risk management approaches, rather than a component to be slotted into or tacked onto an existing organization. It is also not a fixed approach, but a mindset that must adapt as new possibilities come along. We must be continually vigilant that we do not make our businesses accidentally fragile in the service of the gods of efficiency. We must continually and deliberately manage the tension between efficiency and antifragility; although some business moves will increase both, some represent a trade-off.

For IT/digital leaders, antifragility should become an important topic. First, because many of the aspects of antifragility are facilitated by IT-related capabilities, such as a move to the cloud, DevOps and microservices, architecting for more modular business models, and increased trading and collaboration (e.g. in ecosystems and platform businesses). And second, because several of the new risks and stressors emanate from the IT/digital world, such as cyber-risks and risks related to higher levels of automation.

The adoption of services available in the Matrix/the public cloud is closely aligned with the goal of antifragility, in ways such as an aggressive approach to both mainstream adoption of core cloud services and early experimentation with new value-added service.

We recommend that CIOs keep antifragility in mind, and run through the nine stratagems listed above in all strategy and planning activities, continually looking to discuss antifragility at the senior leadership level, and build more antifragile businesses. At LEF, we believe that this concept of antifragility ‘has legs’, and will continually build this thinking into our work with clients and our thinking on Winning in the 21st Century.
Evolution 75 Silk is an FSC certified recycled paper and board range manufactured using 75% post consumer recycled fibre and 25% virgin fibre of which 70% is FSC certified. Evolution 75 Silk carries the FSC Mix label.

© 2017 DXC Technology Company. All rights reserved.