Anti-Fragile Information Systems

Completed Research Paper

Arnaud Gorgeon
Groupe ESC Clermont - EA3849, CRCGM
4, Bd Trudaine – 63037 Clermont-Ferrand Cedex 1

arnaud.gorgeon@esc-clermont.fr

Abstract

As complex socio-technical systems composed of many interconnected parts, interacting in non-linear, dynamic, emergent and often unexpected ways Information Systems are fragile. In this paper we introduce the concept of antifragility as an alternative mean of apprehending the fragility of Information Systems and a novel way of dealing with risk, uncertainty and the unknown. Antifragility is the opposite of fragility. Antifragility allows to go beyond robustness or resilience by moving away from a predictive mode of thinking and decision making to a mode that embraces the unknown and randomness and focuses on the characteristics that render systems fragile rather than trying to assess and predict the chain of events that may harm them. We propose a set of guidelines for moving from the fragile toward the antifragile, and explore, for the processes of the IS function, their applications and the questions they raise for practice and research.

Keywords: antifragility, information systems, fragility, robustness, uncertainty, unexpected, processes

Introduction

What can break, will break, and Information Systems are not immune to this adage. As complex socio-technical systems (Bostrom and Heinen 1977), composed of many interconnected parts, interacting in non-linear, dynamic, emergent, and often unexpected ways (Orlikowski and Hofman 1997, Lassila and Brancheau, 1999), Information Systems are fragile indeed. Their fragility is most apparent in the way they fail (Lyytinen and Hirschheim 1987, Doherty et al. 2011). While failure is often of no or little consequence, easily contained, and with little impact, it can at times have dramatic financial, human, and organizational consequences (Nelson 2007). Fragility is first present in the technological artifacts we build: While they are more and more reliable, hardware and software still fail (Bird et al. 2014). Fragility also stems from the methods, models, and structures we develop and use to design, develop, build, implement, and manage Information Systems: many IT projects still run overtime and over budget; users are dissatisfied and do not use systems; needs and expectations are not met; and systems security is still very often breached.

Behind the fragility of Information Systems, and that of most systems, for that matter, lies our inability to predict the future (Makridakis et al. 2009, Makridakis and Taleb 2009a and 2009b, Makridakis et al. 2010). All along their life cycle, Information Systems are indeed vulnerable to the volatility, variability, uncertainty, randomness, and disorder of their internal and external environments. The current methods and strategies used by organizations to mitigate this "cluster of disorder," (Taleb 2012) while increasingly sophisticated, only provide partial solutions. Organizations perform risks assessments (Smith et al. 2001); they strive to reduce the vulnerability and increase the reliability (Butler and Gray 2006) and the resilience of their systems (Wang et al. 2010). But all these methods have the underlying assumption that harmful events are known and their occurrence and their effects can be assessed. At best, Information Systems reach a satisfactory level of robustness or resilience, but they are only robust or resilient to known past conditions and remain fragile to unpredictable and unforeseeable ones.

If anticipation and prediction are illusory, is there any hope then for organizations to be able to design, develop, build, implement, and manage Information Systems that are less fragile to their increasingly complex and unpredictable internal and external environments?

To answer this question, we introduce in this paper the concept of antifragilty as an alternative means of apprehending the fragility of Information Systems and a novel way of dealing with risk, uncertainty, and the unknown. Antifragility was developed by Nassim Taleb in his book Antifragile: Things that Gain from Disorder (Taleb 2012). Antifragility is the opposite of fragility.[1] While we often think of robust, solid, or resilient as antonyms of fragile, these notions lie in fact in the middle of the fragile–antifragile continuum, as does neutral between positive and negative. The Fragile suffers from the volatility and uncertainty of its environment; it is easily broken or destroyed. The Robust doesn't care; it remains the same. The Antifragile is not only robust but it also benefits from volatility and uncertainty; it improves under stress. Start-up e-commerce websites, for instance, are often fragile to security breaches, traffic peaks, and the growing complexity of their interacting and serving customers. Established sites, such as Amazon or eBay, have proven to be robust and resilient in these areas. A fully autonomic e-commerce site would be considered antifragile if it could be capable of automatically and securely adjusting and improving its advertising, product, and service offerings according to the variations of interactions with its customers and the disruptions caused by its competitors and other stakeholders.[2]

Antifragility extends the continuum of fragile–robust and opens up a domain where randomness, chaos, volatility, uncertainty, etc. become sources of improvement rather than elements one seeks to minimize, master, or even eliminate. Antifragility, we will see, allows us to go beyond robustness or resilience by

[1] Taleb (2012) coined the word antifragile as he could not find in all the languages he investigated a word for the antonym of fragile.

[2] Initiated in 2001 by IBM (Kephart and Chess 2003), autonomic computing aims to develop systems capable of adapting to unpredictable changes in and to the growing complexity of their operating environments by self-configuring, self-healing, self-optimizing, and self-protecting themselves.

moving away from a predictive mode of thinking and decision making to a mode that embraces the unknown and randomness and focuses on the characteristics that render our systems fragile rather than trying to assess and predict the chain of events that may harm them.

The concept of antifragility has been explored across many disciplines. In Engineering, for instance, Johnson and Gheorghe (2013) propose a framework for analyzing and measuring antifragility based on a system of systems concepts. They apply their framework to analyze the risks associated with space weather on the U.S. smart grid electrical system. In Finance, White (2013) explores the fragility of banking and monetary systems and discusses ways of rendering them antifragile. In Computer Science, Tsetlin (2013) presents how at Netflix, antifragility is used as a strategy for the prevention and management of software and system failures in large-scale distributed systems. Abid et al. (2014) propose a solution to design antifragile systems in cloud computing environments, and Guang et al. (2014) propose an antifragile development process for cloud computing on public infrastructures under the contradicting interests of users, companies, and governments. To our knowledge antifragility has not yet be formally discussed in our field. We believe, however, that antifragility may help our practical and theoretical understanding of how organizations can design, build, implement, and manage their Information Systems in increasingly complex and unpredictable environments. We suggest that Information Systems must be more than just robust or resilient—they must become antifragile.

We begin our discussion by presenting the concept of antifragility, showing how it extends the fragile–robust continuum. We then argue the need to stop trying to predict events that can harm our systems and assessing their fragility instead. We continue our discussion by proposing a set of guidelines for moving from the fragile toward the antifragile. Finally, we present a simple framework to explore the relevance of these guidelines to the monitoring, core, and enabling processes of the IS function, with the underlying aim of revealing unexplored questions for practice and research.

The Triad: Fragile–Robust–Anti-fragile

Over their life span, systems are exposed to what Taleb (2012) calls the "disorder cluster": uncertainty, variability, imperfect and incomplete knowledge, chance, chaos, volatility, disorder, entropy, time, the unknown, randomness, turmoil, error, dispersion of outcomes, and unknowledge. Fragile, robust, and anti-fragile systems react differently when exposed to this cluster.[3]

Fragility. Fragile systems suffer from it; they are easily broken or destroyed, and are thus vulnerable. The survival of these systems is heavily dependent on things following their planned course, and one must anticipate their behavior.

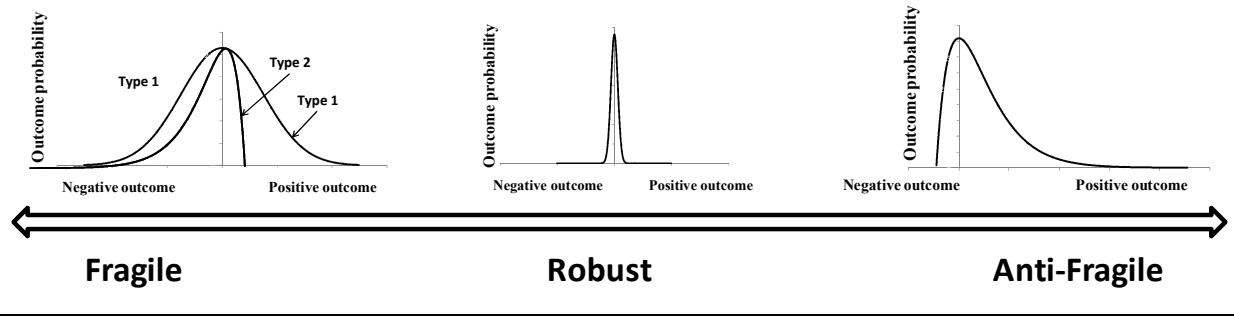
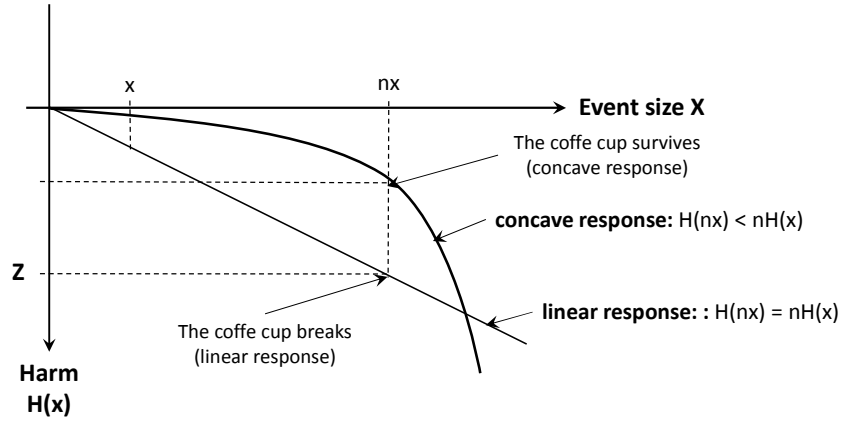


Figure 1. The Triad: Fragile–Robust–Antifragile and their outcome distributions when subjected to stress (based on Taleb [2012])

[3] In the reminder of this paper, we shall interchangeably use the words harm, stress, volatility, uncertainty, etc. to refer to the "disorder cluster" when there is no risk of misinterpretation.

Taleb (2012) distinguishes between two types of fragility. The first, referred to as Type 1, may produce both large positive and negative outcomes. Type 1 fragility is found in most Information Systems; they can indeed create extraordinary value, but they may also fail in catastrophic ways. Type 2 fragility only potentially induces large negatives outcomes. IS security, for instance, is typically subject to this type of fragility. One of the main characteristics of fragile systems is that they exhibit a negative outcome probability distribution with a thick left tail (see Figure 1), at the end of which lurk very rare—and as such extremely difficult to predict—catastrophic outcomes. Some systems we thought robust proved to be fragile, and many fragile systems are believed to be robust because they have never broken (e.g., the Internet, see Buldyrev et al. [2010]). Fragility is also context dependent; something may be fragile in a particular environment and not in another.

Fragile systems necessarily respond to stress in a non-linear fashion. This non-linearity resides in the fact that fragile systems withstand very well small variations, but the compounded effects of these small variations never lead to their breaking point; otherwise, most systems will never survive. A coffee cup resists thousands of small shocks during its life time and survives. Fragile systems thus exhibit a concave response to harmful stressors (see Figure 2 below). The more concave the harm function, the more harm from the unexpected—and disproportionally so. For instance, commuting time in Los Angeles is fragile to traffic, and exhibits a non-linear response to the number of cars circulating on its freeways. Traffic is fluid up to a point but may come to a halt simply by adding just one car. Fragility is thus defined as a *concave* sensitivity to a stressor or a source of harm, leading to a negative sensitivity to increases in volatility, disorder, etc. (any element of the disorder cluster) (Taleb and Douadi 2013).



Taking x as the stress level and H(x) as the harm function, for n>1, H(nx) < nH(x) for all 0 < nx < Z, where Z is the level (not necessarily specified) at which the item is broken.

Fragility is defined as a ***concave*** sensitivity to harmful events, leading a negative sensitivity to increases in stress, volatility, etc. (Taleb and Douadi 2013)

Figure 2. Concave response of fragile system to stress (based on Taleb [2012])

Robustness. Robust systems are indifferent to the "disorder cluster"; they remain the same, up to a point (everything breaks ultimately given the right conditions). Resilient systems may change but will recover their original state.[4] Robust or resilient systems do not gain or lose anything from being exposed to the "disorder cluster," and when exposed to it, the distribution of possible outcomes is thus relatively narrow (see Figure 1).

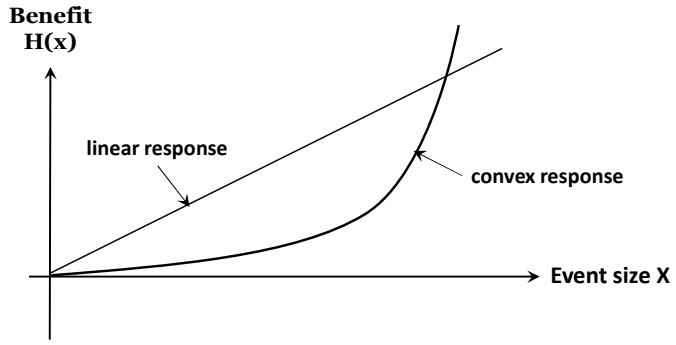
Antifragility. Antifragile systems benefit from the members of the "disorder cluster." For instance, by allowing a small fraction of its devices to be infected, a networked system (i.e., cell phones) can be made antifragile to infectious malware with unknown and time-varying spreading mechanisms. Imperfect

[4] In this paper, we adhere to the etymological definition of resilience: to spring back and rebound (from the Latin verb resilire). The management and psychological literature has unfortunately extended the concept of resilience to include the notion of springing forward and improving, adding confusion to an already confusing concept (see Müller [2013] for a discussion of resilience in IS).

malware detection then quickly increases the system's resistance to malware spreading by increasing software diversity where the infections were detected (Hole 2015).

The Greek mythology has its own antifragile creature, the Lernaean Hydra, the reptilian monster whose many heads grow back manifold when cut off. As the opposite to fragility, antifragility is defined as a *convex* response to a stressor or a source of harm (see Figure 2), leading to a positive sensitivity to increases in volatility, disorder, etc. (any element of the disorder cluster) (Taleb and Douadi 2013). For antifragile systems, positive outcomes largely outweigh negative ones, which yields a distribution largely skewed to the right, where large positive outcomes are possible and much more favorable that negative ones (see Figure 1).

Paradoxically, antifragile systems rely on the fragility of their sub-components. Fragile elements must indeed disappear to give place to better ones so the system can improve. A system without fragile sub-components is merely robust; it will not improve following the disappearance of its fragile parts. The antifragility of our transportation systems (i.e., cars, planes, or boats) rests on the fragility of its components. Each accident triggers improvements making the system as a whole safer.



Antifragility is defined as a ***convex*** response to harmful events, leading to a positive sensitivity to increases in stress, volatility , etc. (Taleb and Douadi 2013)

Figure 3. Convex response of antifragile system to stress (based on Taleb [2012])

Lastly, antifragility must be distinguished from flexibility and agility. Both concepts are often evoked as essential characteristics of systems facing rapid change, uncertainty, and unpredictable environments. Flexibility represents a combination of adaptive dynamic capabilities, allowing an organization to adapt and adjust quickly in advance to environmental change (Teece et al. 1997, Volberda 1996). Flexibility allows the organization to prepare and reconfigure itself for change before it occurs. Agility extends the concept of flexibility in providing the organization with the ability to sense and to respond to unexpected change by rapidly reconfiguring itself (Dove 2001; Sambamurthy et al. 2003, Overby et al. 2006). While flexibility and agility may contribute in some ways to antifragility (this will have to be further investigated), the two concepts fundamentally deal with adaptation in the face of uncertainty. Antifragility, however, is about improvement.

From Prediction to Anti-fragility

Organizations continuously look ahead to the future. They have to plan for resources, to manage risks, to forecast capital and operational expenditures, and to develop and predict the adoption of new goods and services, to cite but a few examples. The IS function also has some specific forward-looking tasks of its own: It has to answer the question of "whether, when, and how to innovate with IT" (Swanson and Ramiller 2004) to manage, develop, and implement new systems and predict their impacts on their organizations.

Looking toward the future involves making predictions and forecasts judgmentally, quantitatively, or both (Bunn and Wright 1991). To tame uncertainty and the unknown, organizations increasingly rely on experts and sophisticated predictive and forecasting qualitative and quantitative models and methods.

Taleb (2012), Makridakis et al (2009), and Goodwin and Wright (2010) have identified, however, severe shortfalls with these methods.

The first is that the future is never exactly like the past. History has indeed shown us that there are no such things as typical successes or failures. Major events, positive or negative, are unique. Nobody predicted the latest financial crises, the Fukushima disaster, or the success of Google—at the end of the 1990s the founders of Google tried to sell the company for $1.6 million (Battelle, 2005). Lack of data impedes reliable assessments of the underlying probability distribution of possible events. Extrapolation based on past patterns or relationships which may exclude possible extreme events cannot provide accurate predictions.

Second, statistical models work well if the assumptions about the probability distributions are correct. A Gaussian view of the world unfortunately pervades most of the research and practice (Andriani and McKelvey 2009). In real life, however, thin-tailed distributions (e.g., Gaussian or Poisson), with finite variance and stable means, are found only in rare places, such laboratories and casinos. Organizational and economic life do not belong to the Gaussian world but rather exhibit power-law distributions with unstable means and infinite variances (Andriani and McKelvey 2009). Simplifications often made in the representation of real systems often do not fully account for the complex interactions between elements. In real life, events are rarely independent, and model errors are often not tractable.

Third, we have very often little or no knowledge about the nature of the distributions of events that can affect systems, positively or negatively. And, since complex systems react mostly in a non-linear fashion to harmful stressors, outcomes distributions very often have very little in common with the distribution of harmful events. A Gaussian distribution is easily transformed into a fat-tailed distribution via a non-linear function, for instance.

Lastly, research has shown extensively that decision makers use heuristics to cope with the complexities of estimating probabilities (Tversky A. & Kahneman 1974). While these heuristics often ease the decision process, they also have been shown to systematically bias judgment. Heuristics that affect judgment are many, and we discuss next some of the most representative. The availability bias leads to the assignment of a higher probability of occurrence to recent, vivid, or unusual events (Tversky and Kahneman 1973). Conversely, rare events or events that never occurred will be assigned a zero or near-zero probability. The representativeness heuristic leads people to underestimate the base rate frequencies of events. Decision makers tend to see their forecasting problem as unique and tend to ignore the larger class of similar events, relying instead on low-validity, individuating information (Kahneman and Lovallo 1993). Lastly, anchoring and insufficient adjustment (Tversky and Kahneman 1974) may lead forecasters to make insufficient adjustments to their current estimations when estimating the future.

So, "What can we do in a world increasingly complex and uncertain; in a world we struggle to or cannot understand?" Taleb asks. As an answer, Taleb proposes that one should focus on assessing the fragility of systems and forget trying to assess the occurrence of harmful events that may harm them. Rather than asking, "Why didn't we see these events coming?" we should ask: "Why did we build something so fragile to these types of events?" We should focus on outcomes rather than their causes; we rarely observe the events at the root of positive or negative outcomes, especially for rare extreme events. What we more easily observe, however, are the outcomes themselves. It is impossible, for instance, to predict the occurrence of the next earthquake that will hit Tokyo, but we can build an environment that will resist it. We do not know when the next cyber-attack may affect a system, but we can build it so it will resist it. Most of the time, we have no control over the events that may harm our systems, but we have much more control over the harm that can be done. This change of focus, from trying to predict harmful events to rendering systems antifragile, is key to operating in a world that is increasingly complex and uncertain. Taleb (2014, p. 7) summarizes this point stating that "It is more rigorous to take risks one understands than try to understand risks one take."

The definitions of fragility and antifragility implicitly contain a simple heuristic to assess whether a system is fragile or antifragile: All we need to know is whether the system is accelerating toward harm or benefit when submitted to stress. We do not need to know the history or the statistical behavior of a system, nor do we need to be able to predict the events that may harm it (Taleb 2012).

Anti-Fragile Information Systems: Some Guidelines

In his book, Taleb (2012) explicitly discusses the factors that are key to moving a system from the fragile to the antifragile domain. These factors focus on two aspects, namely, reducing fragility and harnessing

antifragility. In this section, we discuss the elements we have selected as the most appropriate ones to serve as guidelines for antifragile Information Systems. While we will discuss sociotechnical systems in particular, with an implicit focus on organizations and their Information Systems, the guidelines we propose may also apply to other types of systems.

Simplicity

Driven by globalization, the customization of their products and services, and an increasing information processing needs, organizations and their Information Systems have grown more complex over the years (Galbraith 2012, 1972). They are fragile because the number and variety of their constitutive elements together with the dynamics of their interactions and interdependencies make them difficult to apprehend cognitively as a whole, and their non-linear emergent behaviors are very often very hard, if not impossible, to predict.

Complexity is pervasive in the way we design, develop, implement, and manage Information Systems, and, not surprisingly, Complexity Theory is permeating our field as a mean to understand it.[5] While our academic research and discourse acknowledge complexity, simplicity has been relatively ignored.[6] This is surprising, because if complex systems are fragile, simplifying them should be an important aim. We found very few instances of research on simplicity in our field. Schneberger and McLean (2003) are among the rare researchers who discuss ways of reducing Information Systems complexity. The authors propose three fundamental approaches to simplifying computer systems: simplify individual components and combine them into larger virtual ones; use fewer and more standardized components, reduce their independencies, and slow the rate and frequency of the system change; and distribute entirely centralized systems and increase the centralization of entirely distributed systems. Modularity and standardization are thus key principles of simplicity which have been largely exploited in our field at the technical level.

As a key element of design (Maeda 2006), simplicity has also been explored in the context of the design, use, and adoption of socio-technical systems. Trier and Richter (2013), for instance, explore the role of simplicity in the adoption and use of corporate social software. Nadkarni and Gupta (2007) showed that complexity (taken here as the antonym of simplicity) had a negative impact on user satisfaction with websites. Using the Technology Acceptance Model (TAM), Lee et al. (2007) show a positive relationship between simplicity and perceived ease of use in blogging services.

Taleb (2012) offers a complementary perspective on simplicity. For Taleb, simplicity is first about subtraction. Drawing from Popper (1959), Taleb argues, for instance, that knowledge grows more from subtraction than it does by addition. We learn more from negative knowledge (what we know doesn't work or to be wrong) than from positive knowledge (what we think work or to be right), because what is wrong today cannot be right tomorrow, whereas what we think is right today may turn out to be wrong tomorrow. Subtraction is also removing the bad from a system, such as harmful elements or people, to reduce fragility and enhance antifragility. As Saint Exupery said, "Perfection is achieved not when there is nothing more to add but when there is nothing left to take away." Avoiding unnecessary interventions, a principle we shall discuss later in detail, is also a mean of letting a system take care of itself and exercise its natural antifragility (Taleb 2012).

Simplicity also lies in the aphorism of less is more (Taleb 2012). For instance, in forecasting, simpler methods have proven to work better than complex ones (Makridakis et al. 1979; Makridakis and Hibon 2000). Fast and frugal heuristics also often work better than complex models of decision making (Gigerenzer and Goldstein 1996). In statistical models, fewer parameters reduce the weight of noise and

---

[5] A review of the existing literature on the topic goes beyond the scope of this paper. As an example, the Journal of Information Technology and Information Technology and People devoted special issues to Complexity Science in our field; see Merali and McKelvey (2006) and Jacucci et al. (2006) for an overview.

[6] A search for the terms "Information Systems" and "complexity" in the body text of peered reviewed articles in the EBSCO and PROQUEST databases returns over four times more articles than a search for "Information Systems" and "simplicity."

random errors, leading to better predictive models. In all, Taleb (2012) suggests that simplicity is a powerful and more efficient way to apprehend the complexity and uncertainty of our environments. As a result, when exercised, simplicity, in all its forms, has not only the potential of reducing the fragility of systems but also the power of enhancing their antifragility.

Skin in the Game

Organizations are increasingly complex and specialized and thus difficult to control (Vaughan 1983). In such an environment, information opacity and asymmetry arise and are conducive to moral hazard. Moral hazard can be defined as "any situation in which one person makes the decision about how much risk to take, while someone else bears the cost if things go badly" (Krugman 2009). Moral hazard is a source of fragility for organizations because they potentially suffer the downsides of risky decisions made by a few who in the process create high potential upsides for themselves and become more antifragile.

As an antidote to moral hazard (beyond that of classical insurance schemes), Taleb (2012) and Taleb et al. (2014) proposes that managers, planners, forecasters, decision makers, and opinion makers in general should all have some exposure to the decisions they make. They should have "skin in the game" —that is, they should bear some or all of the cost, whether positive or negative (physical, emotional, financial, etc.), of their risky decision making. Borrowing from the Babylonian Code of Hammurabi, which dates from circa 1772 BC, Taleb exemplifies the idea of skin in the game quoting the following law:

> "If a builder build a house for someone, and does not construct it properly, and the house which he built falls in and kills its owner, then that builder shall be put to death."

The Babylonians understood well that the builder knows more than anybody else about the risks associated with the defects of his construction and that he can hide them from potential buyers and inspectors. While the incentive, or better said disincentive, may seem extreme, the law clearly exemplifies the idea of exposing oneself proportionally to the risk taken. Many professionals have skin in the game: entrepreneurs, writers, artists, independent traders, and airplane pilots, for instance. In organizations, however, the questions arise as to how much skin in the game organizational actors really do have and should have.

We found very little research dealing with moral hazard in our field. In one notable paper, Tuttle et al. (1997) conducted a decision-making experiment showing that experienced IS professionals have the tendency to implement an IT project with quality problems in a moral hazard situation. The authors found that, shielded from top management attention, IS professionals preferred to implement a project with quality problems rather than delay its implementation and lose a substantial part of their usual compensation. Interestingly, they found, however, that ethical considerations from IS professionals could mitigate this behavior.

Reduce Naïve Interventions

Taleb (2012) argues that we often underestimate the natural antifragility of systems and that we need to be aware of the fragilizing effects of our interventions. Many systems indeed have an innate ability to take care of themselves. For Taleb (2012), the problem is not intervention per se—under-intervention can be as harmful as over-intervention. The issue is with naïve intervention—that is, the lack of awareness and acceptance of the harm done by it. Examples of naïve interventions are probably most prevalent in the medical field. Iatrogenesis[7] (preventable harm caused by a medical treatment or advice to patients) may kill 225,000 people a year in the United States, constituting the third leading cause of death after heart disease and cancer (Starfield 2000). The medical field has even adopted the term "technological iatrogenesis" to characterize the harm done by the introduction of innovative technology in complex health care systems (Palmieri et al. 2007).

At the heart of the matter lies the question of when to intervene and when to leave the system alone. According to Taleb (2012), one way to reduce naïve interventions is simply not to intervene at all or to

[7] Greek term, meaning "brought forth by the healer."

delay the intervention itself, letting the system take care of itself and exercise its natural antifragility. However, doing nothing is rarely acceptable; and as Taleb (2012) notes, organizations rarely reward those who by *not* doing bring value or avoid harm to their organizations. Organizations tend to reward rather those who do—the achievers.

However, doing nothing or delaying action may actually bring some value. Tired of seeing new managers bringing about change in their newly acquired zone of influence to legitimate their worth, the Global Head of Human Resources at Zurich Financial Services, prohibited them from changing anything for a year (Clark 2013). Known for the efficiency of its production systems, Toyota paradoxically uses a "wait and see" approach for the development of its new cars. To develop new models, Toyota explores a large number of prototypes in parallel and delays the setting of the final car body shape as much as possible and the releasing of the final specifications to their suppliers until late into the design process, allowing them to explore and improve alternatives (Ward et al. 1995). Closer to home, hackers develop stalling codes to delay the execution of the malicious activity long enough so that an automated dynamic analysis system fails to extract the malicious behavior (Kolbitsch, 2001).

"Festina lente," make haste slowly, encapsulates well the principle of reducing naïve intervention. Antifragility implies that the old is superior to the new (Taleb 2012) simply because it has survived the test of time, while the fragile has not. Doing nothing or delaying action is a way to respect the old or give it the time to exercise its natural antifragility.

Optionality

Optionality, the availability of options, allows systems to benefit from the positive side of uncertainty without suffering serious harm from the negative side (Taleb 2012). In the face of uncertainty, to have the option but not the obligation to engage in a course of action is a source of antifragility (Taleb 2012). Complex socio-technical systems are fragile because anticipating and understanding their behavior is difficult, if not impossible. Establishing cause and effect relationships among system components is indeed out of reach due to the sheer number and diversity of the components involved. Optionality reduces the need to understand or forecast the future with accuracy and only requires having the wisdom and rationality of choosing the option that will be favorable. Furthermore, choice can be based on assessments made after the outcome of an adverse event and not beforehand (Taleb 2012).

The notion of optionality has been extensively exploited in finance through the option, a contract offering the right, but not the obligation, to buy (call) or sell (put) a security or other financial asset at an agreed-upon price during a certain period of time on a specific date. The theory of real options has adapted the techniques developed for financial options to capital investment decisions for uncertain projects. Real options provide organizations the analytical tools to shift from thinking about what they must do on a project to what they may do (Fichman et al. 2005). In our field, Real options have essentially been used in the realm of IT project investment management (e.g., Fichman 2004 and Benaroch and Kauffman 1999). We consider next two other sources of optionality organizations may exercise when they face uncertainty: experimentation in the form of trial and error and selectionism (Pich et al. 2002) and redundancy.

Trial and error create variations and thus optionality through learning. Learning is achieved by actively searching for new information and flexibly adjusting activities and targets to this new information, applying new and original problem solving as new information becomes available (Sommer and Loch 2004). Trial and error not only creates new knowledge and insights but also allow the system to improve beyond the status quo through a better appreciation and understanding of what works and what doesn't and, more importantly, of what can fail or not. Nature is antifragile because it has evolved through trial and error for billions of years (Simonton 1999). What was meant to break broke, and the rest evolve into something better. Selectionism refers to trying multiple solutions in parallel and selecting the best ex post (Sommer and Loch 2004). Trial and error learning, selectionism, and other forms of experimentation are the fuel for innovation and are extensively used in very specific areas of organizations, such as R&D, product design, and test marketing, but are very rarely authorized by administrators in others domains (Huber 1991). In our field, prototyping and pilot implementation are typical means by which to experiment with new systems (Hertzum 2012; Janson et al. 1985).

Another source of optionality is redundancy. Redundancy comes in two forms: redundant parts and redundant functions (Emery 1967). In biological and engineering systems, redundancy of parts consists of

multiplying the number of critical components to increase reliability. Natural systems have developed redundancy as part of their way of managing risk and the unexpected. The human body has many redundant parts (two lungs, two kidneys, etc.), for instance. In our field, redundancy is largely exploited; data and computational replication, for instance, aim at improving accessibility, reliability, and fault-tolerance. In organizational life, redundancy of parts consists of multiplying specialized units across an organization. IT support, for instance, may be decentralized within each business unit. In organizations, redundancy of functions consists of adding functions to each organizational unit so that they are each able to perform a range of functions instead of a single, specialized activity. For instance, employees may be trained to learn several jobs and be available to replace others if need be. While redundancy contributes to a system's robustness and resilience, it is also a source of antifragility. Redundancy, in the form of extra cash, for instance, may allow an organization to benefit from the volatility of its environment to invest in promising opportunities, and extra inventory may facilitate the exploration of new markets (Taleb 202). Redundancy has, however, a direct and an opportunity cost that organizations rarely have the desire to bear in the name of optimization and efficiency. Redundancy may also have the perverse effect of increasing complexity, raising the likelihood of failure (Perrow 1984).

Inject Randomness into the System

In their managing of uncertainty, organizations strive to remove noise, randomness, and volatility from their operations and environments. Standardization, norms, procedures, risk analyses, feasibility studies, etc. are useful tools, but the illusion of stability, control, and safety that their use ensues is a source of fragility, because silent risks inevitably accumulate below the surface, and ultimately the unexpected always happens. Taleb (2012) argues that randomness and volatility are the fuel for antifragility: They unlock inertia and create surprises, leading to opportunities to learn, to evolve, and to improve. Using agent-based simulation, Pluchino et al. (2011a), for instance, showed how the injection of a measure of randomness into the selection of politicians improves the efficiency of a parliamentary institution. The same authors also showed that in a pyramidal organization, random promotion increases organizational efficiency (Pluchino et al. 2011b). Closer to home, Netflix developed a series of software, the Simian Army (Chaos Monkey; Chaos Gorilla, etc.), which randomly tests the resiliency and recoverability of their systems (Tseitlin 2013).

While organizations treat randomness with suspicion and anxiety, it has benefited many to extraordinary extents. Randomness is indeed at the heart of serendipity, which has been at the source of many of the greatest and most lucrative discoveries of the latest century (Harré 2012).

Decentralize / Develop Layered Systems

Decentralization and developing layered systems have the same main objective: the contention of the effects from harmful events. As Taleb (2009, p. 163) mentions: "The idea is simply to let human mistakes and miscalculations remain confined, and to prevent their spreading through the system, as Mother Nature does."

In our field, decentralization has been explored across various domains. The first is IT governance. There is no best universal structure for IT governance (Brown and Grant, 2005), and IT governance structure may be looked at as belonging to a continuum from being totally centralized, where all IT resources are allocated to a single unit which provides the entire organization with IT services, to being entirely decentralized, where all IT resources are allocated to individual business units that use those resources to satisfy their own needs independently (Gordon and Gordon 2000). The extant research suggests that organizations tend to decentralize IT governance in more uncertain environments (e.g., Brown 1997). As regards their IT infrastructure governance, Xue et al. (2011) show that organizations respond to uncertainty in a more complex manner. They tend to decentralize their infrastructure when environmental uncertainty increases but centralize it as uncertainty increases further. Decentralization has also been explored in the context of data management. Velu et al. (2013) propose, for instance, a framework to help managers decide whether to centralize or decentralize their data management according to the level of uncertainty and the similarity of their business units. They found that organizations should decentralize their data management under two conditions: when their business units are similar and uncertainty is high and when their business units are dissimilar and uncertainty is low.

Paradoxically, antifragile systems rely on the fragility of their components, without which they would be merely robust. Under stress, these fragile subcomponents break, allowing the system to improve. Every fraud on the Internet makes the system a lot safer. Layered systems are arrangements in which components interact in a hierarchical and sequential manner; components from one layer usually interact only with components of a neighboring layer, providing potential damage confinement. Layered approaches to systems are ubiquitous in our field, and we found them in Enterprise Architecture and Service Oriented Architecture (SOA) frameworks, the Internet, and many software architecture designs (e.g., multilayer software architecture).

Antifragility and the IS Function Value Creation Processes

In this section, we propose a framework to explore the relevance of the guidelines we have just discussed to the value creation processes of the IS function (Agarwal and Sambamurthy 2002). Our aim is twofold: to structure the elicitation of new and relevant questions for research and practice and to stimulate exploration across domains. Indeed, we believe that the intriguing idea of improving under stress may generate some interesting theoretical discussions in many areas of our field and offer some practical solutions to managing IS in the face of uncertainty and the unexpected. Also, as we have seen, while some of the antifragility guidelines we presented are already applied in some areas of our field, their applications remain very domain-specific, and they do not appear to have crossed many boundaries. The framework we propose should help reduce this domain dependence and offer opportunities to explore these guidelines in unfamiliar domains. For instance, simplicity is a key design principle, but what does simplicity means for the way we manage IT support or IS investment?

Figure 4 below shows a typical process map of an IS function, acknowledging that such a map is unique for each organization. Borrowing from Agarwal and Sambamurthy (2002) and the COBIT 5 Process Reference Model (ISACA 2012), we differentiate among three kinds of processes: the enabling or support processes, the core processes, and the monitoring processes. The enabling processes create value for customers internal to the IS organization. They typically regroup processes such as the management of human capital, risks, security, quality etc. The core processes create value for customers of the IS function. They typically include processes such as the provision of services and solutions together with the definition of the enterprise architecture. Lastly, the governance or monitoring processes represent the processes by means of which the IS function is run. A more detailed description of these processes is provided in Appendix 1.

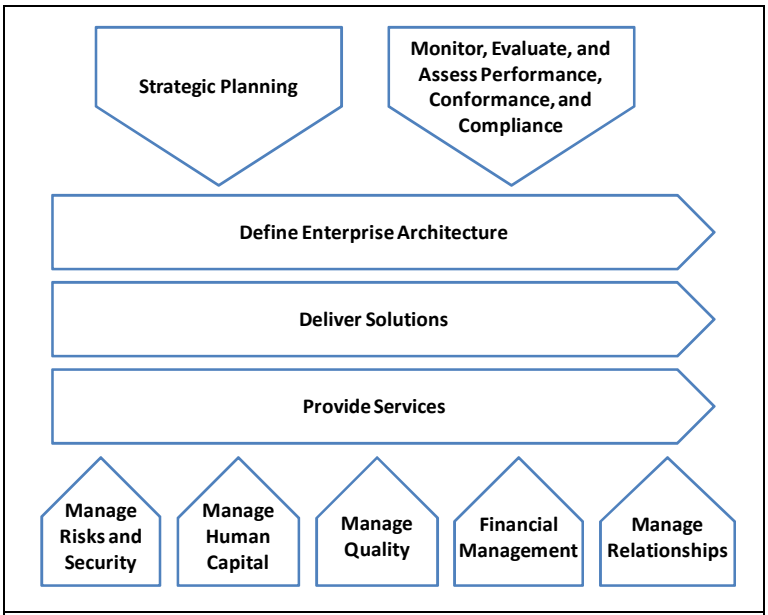


Figure 4. Typical IS processes of the IS function

Crossing the IS function processes with the antifragile guidelines led to the table shown in Appendix 1. The table may be used as a probing tool to question for each process of the IS function the usefulness and applicability of the guidelines we have proposed. The aim is also to reveal unexplored questions for research and practice.

As an example, we explore next what the antifragile guidelines can mean for the "strategic planning" process of the IS function. We take the points of view of the CIO and the top management team, which, together, have the challenging task and the final responsibility of identifying and exploiting IT-related opportunities that create business value. Following Chen et al. (2010, p. 235), we define IS strategy as "the organizational perspective on the investment in, deployment, use, and management of information systems," which recognizes not only the formal but also the processual, implicit, and emergent nature of IS strategic planning. At the end of our discussion, we propose a sample of questions (see Table 2), which emerged during our exploration, for research and practice.

Simplicity.

As we have argued, simplicity possesses not only the potential of reducing the fragility of systems but also the power of enhancing their antifragility itself. Seen as the reduction of the numbers of elements in a system, simplicity is well understood by the IS function, which strives to achieve standardization, integration, and modularity and to reduce the number of applications, data centers, or equipment vendors, for instance. While these simplifications may reduce the complexity of IS and hence its fragility, they do not always bring simplicity to business activities, and they may even rigidify the organization and fragilize it. For simplicity to be effective, we suggest that it should go beyond IS function boundaries and permeate the entire organization. Simplicity should therefore be a part of the reflections conducted by the IS strategic planning committee as a whole. It should be defined by the business stakeholders and then translated by the IS function into strategic IT initiatives with measurable simplicity objectives of their own. In all, the ineluctable growth of IT complexity should serve the simplicity of the business, and one focal question IS strategic committees should answer is "how can IS support and enhance the simplicity of the value creation activities of the business?"

Skin in the game.

"Skin in the game" should prevent organizational actors from making risky decisions that can fragilize their organization by making them bear some or all of the cost, whether positive or negative, of their decision making. Disincentives, such as loss of compensation (i.e., bonuses, benefits, or equity) or even termination of employment, are strong deterrents, but they rarely balance the loss an organization may incur from inadequate decision making. IT vendors and outsourcers have "skin in the game" because their contractual relationship with their clients (i.e., Service Level Agreement [SLA]) often includes penalty clauses commensurate with the losses they may induce. The IS function often sets SLAs with its internal customers, but these very rarely include similar penalties. We have never heard of a case in which the business has compensated the IS function for its liability in a failed project. IS strategic initiatives often continue to fail. The question of whether IS strategic project stakeholders have enough "skin in the game" is a legitimate question that IS and business executives should ponder on. If the answer is no, the challenge will be to find disincentives that are commensurate with the potential losses and that not only ensure the highest level of commitment but also curb the behaviors and prevent the actions that can lead to project failure. This issue is undeniably a controversial one.

Reduce naïve interventions.

Reducing naïve interventions by simply not intervening at all or delaying the intervention itself allows the system to take care of itself and exercise its natural antifragility. One of the difficult tasks IT strategic planning stakeholders often need to make is deciding on which legacy systems to keep or to cut. Many factors may tilt the balance in favor of an upgrade. For instance, the legacy system is expensive to run and maintain, skilled staff is difficult to find, security risks are increasing, business processes have changed, and integration with developing architecture is difficult. Another way to look at legacy systems is that they are no more than systems that have survived and work well; they have proven to be antifragile. Seeking to understand why a legacy system has lasted for so long may therefore be valuable. If legacy systems are antifragile, the IS strategic planning committee should reflect on whether these should be transformed or modernized to the organization's advantage.

The IS function is under pressure not only to deliver the expected customer experiences by harnessing the latest IT innovations but also to keep running reliably back-end transactional processes where most legacy systems are usually found. The compromise to envisage is thus the following: innovating with IT for customer facing systems at the risk of fragilizing the system, as well as taking advantage of the antifragility of those legacy back-end systems that are worth maintaining.

Optionality.

The availability of options allows systems to benefit from the positive side of uncertainty without suffering from its negative side (Taleb 2012). Options are a source of antifragility (Taleb 2012). Multiple scenario planning has long been used by organizations in their strategizing activities. Scenarios are "focused descriptions of fundamentally different futures presented in a coherent script-like or narrative fashion" (Schoemaker 2003, p. 195). In essence, multiple scenario planning is about envisioning options. While scenario planning has been criticized, for many of the reasons we have argued about in relation to our inability to predict the future, engaging in multiple scenario planning may be valuable for the IS strategic planning team. This value of scenario planning is not so much on its outcomes or the production of scenarios but on the results of the social and cognitive processes it entails. Scenario planning forces participants to share and challenge their assumptions, frames of references, and performance criteria (Schoemaker 2003). Envisioning the future collectively creates a shared mental map with which scenario building participants can understand well the future as it unfolds, and it enables the handling of uncertainty in a cognitive and collective manner (Schoemaker 2003). Existing scenario planning methodologies may not be suited to the specificities of IS strategic planning and may need to be adapted to such.

Inject randomness into the system.

Randomness and volatility unlock inertia and create surprises, which in turn lead to opportunities to learn, evolve, and improve; they are the fuel for antifragility. IS strategic planning is an intensive knowledge sharing, learning and social process. Two key areas of this process are the consensual identification of innovative IT-based strategic initiatives and an understanding of their organizational effects that require the sharing and contrasting of novel and different ideas from actors with different requirements and objectives. Randomness can be infused in this process in several ways. It can be first used in the constitution of the IS strategic planning team. While key IS and business executives must be present, a random selection of some organizational members may bring new dynamics to the formal planning process. The lack of relevant knowledge by these randomly selected actors from all organization levels may be compensated by different views and unusual ideas that would have otherwise been overlooked by existing decision makers. Such a random selection can also be used in the constitution of a large IT project management team. Second, random walks by top management across their functional boundaries may also be a way to create opportunities for learning and knowledge sharing through unexpected encounters and discussions. Finally, the temporary random assignment of IS staff to business functions can stimulate the identification of IT-based innovations.

Decentralize.

Taleb (2012) argues that the more centralized a political system is, the more fragile it is. Decentralization makes human mistakes and miscalculations remain confined, and it prevents these from spreading through the system. IT governance represents "the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT" (Weil 2004, p. 3). IT governance forms are shaped by multiple contingencies and belong to a continuum that spans total centralization to total decentralization (see Brown and Grant, 2005 for a review). Interestingly, with the increased consumerization and commoditization of IT, globalization, and the development of web applications, a more decentralized and participatory form of IT governance seems to emerge (Andriole 2015). Most organizations now rely on a much wider range of eternal stakeholders for the management, support, and supply of their IT goods and services. IT vendors, service providers, outsourcers, and even the crowd (i.e. API development) should then be part, to various extents, of the IT governance of their partner organizations. Such a decentralization of power and accountability, across a larger number of stakeholders, may reduce the fragility of the Information Systems they serve.

Table 2. Antifragility and the IS strategic planning process: some questions for research and practice	
Guideline	**Questions**
Simplicity	How do we measure the simplicity of an Information System? How do IS executives understand, implement, and manage simplicity in their organization? How can/do organizations align their business simplicity objectives with those of their IS?
Skin in the game	How much "skin the game" do IS and business executives have in organizations? What disincentives, commensurate with the potential losses, can be used to curb behaviors and prevent actions that lead to IS project failures?
Reduce naïve intervention	Legacy systems have proven to be antifragile; what can we learn from them? How can we transform or modernize legacy systems to our advantage instead of replacing them?
Optionality	What multiple scenario planning methodology is suited to IS strategic planning? To what extant is scenario planning used by the IS function, what methodologies are used, and what impact does scenario planning have on the performance of the organization?
Inject randomness	Does randomness have a place in IS strategic planning, and if yes, in what form? How much serendipity exists in IS strategic planning, and should it be fomented? How does serendipity or other forms of randomness affect the effectiveness and efficiency of IS strategic planning?
Decentralize	How do consumerization and commoditization of IT, together with globalization, affect the IT governance structure of organizations?

The questions we raised in Table 2 represent a small sample of the questions that can be potentially raised when the applicability of antifragility to IS strategic planning is explored. We believe, however, that the few questions which emerged will be of some value. To our knowledge, most of them have not been formally explored or have received very little attention in our field.

Conclusion

In this paper, we have introduced the concept of antifragility. Antifragility extends the continuum fragile–robust and opens up a domain where randomness, chaos, volatility, uncertainty, etc. become sources of improvements rather than elements one seek to minimize, master, or even eliminate. We have argued that antifragility may help organizations to design, develop, build, implement, and manage Information Systems that are less fragile to their increasingly complex and unpredictable internal and external environments. We have proposed guidelines to contain fragility and harness antifragility, suggesting that our attention should shift from trying to predict harmful events to instead focusing on the characteristics that render systems fragile. Fragility and antifragility, as we have seen, can be easily assessed using a simple heuristic: A system accelerating toward harm when submitted to stress is fragile; a system accelerating toward benefit when submitted to stress is antifragile.

We have proposed a simple framework to examine the relevance of the antifragile guidelines to the monitoring, core, and enabling processes of the IT function, with the underlying aim of revealing unexplored questions for practice and research. As we have shown through one particular example, antifragility may raise interesting questions for practice and research.

The concept of antifragility is an emerging concept and needs to be further anchored in existing research; we invite researchers in our field to explore the concept through their respective lenses. While we have proposed some guidelines for antifragile Information Systems, there may be others yet to be to be uncovered. To be useful to theoretical and empirical research, and practice, antifragility and its guidelines will also need to be carefully operationalized.

While much work is required, we believe antifragility offers a promising lens by which to explore how organizations and their Information Systems will face the rising challenges of an ever more connected and complex world driven by globalization and the rapid advances and spread of new technologies, such as Cloud Computing, the Internet of Things, and others to come. We can make one prediction, however: Our inability to forecast the future will likely persist for a while.

References

Abid, A., Khemakhem, M. T., Marzouk, S., Jemaa, M. B., Monteil, T., and Drira, K. 2014. "Toward Antifragile Cloud Computing Infrastructures," *Procedia Computer Science* (32), pp. 850-855.

Agarwal, R., and Sambamurthy, V. 2002. "Principles and Models for Organizing the IT Function," *MIS Quarterly Executive* (1:1), pp. 1-16.

Andriani, P., and McKelvey, B. 2009 "From Gaussian to Paretian Thinking: Causes and Implications of Power-laws in Organizations," *Organization Science* (20:6), pp. 1053-1071.

Andriole, S. J. 2015. "Who owns IT?" *Communications of the ACM*, (58:3), p. 50-57.

Aven, T. 2014. 'The Concept of Antifragility and its Implications for the Practice of Risk Analysis," *Risk* Analysis (35:3), pp. 476-483.

Bird, C., Ranganath, V. P., Zimmermann, T., Nagappan, N., and Zeller, A. 2014. "Extrinsic Influence Factors in Software Reliability: A Study of 200,000 Windows Machines," in *Companion Proceedings of the 36th International Conference on Software Engineering,* Hyderabad, India, ACM, New York, NY, USA, pp. 205-214.

Benaroch, M., and Kauffman, R. J. 1999. "A Case for Using Real Options Pricing Analysis to Evaluate Information Technology Project Investments," *Information Systems Research* (10:1), pp. 70-86.

Bostrom, R. P., and Heinen, J. S. 1977. "MIS Problems and Failures: A Socio-technical Perspective," *MIS Quarterly* (1:3), pp. 17-32.

Brown, A. E., and Grant, G. G. 2005. "Framing the Frameworks: A review of IT Governance Research," *Communications of the Association for Information Systems* (15:1), p. 696-712..

Brown, C. V. 1997. "Examining the Emergence of Hybrid IS Governance Solutions: Evidence from a Single Case Site," *Information Systems Research* (8:1), pp. 69-94.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., and Havlin, S. 2010. "Catastrophic Cascade of Failures in Interdependent Networks," Nature (464:7291), pp. 1025-1028.

Butler, B. S., and Gray, P. H. 2006. "Reliability, Mindfulness, and Information Systems," *MIS Quarterly* (30: 2), pp. 221-224.

Chen, D. Q., Mocker, M., Preston, D. S., and Teubner, A. 2010. "Information Systems Strategy: Reconceptualization, Measurement, and Implications," *MIS Quarterly*, (34:2), p. 233-259.

Chen, P. Y., Kataria, G., and Krishnan, R. 2011. "Correlated Failures, Diversification, and Information Security Risk Management," *MIS Quarterly* (35:2), pp. 397-422.

Clark, D. 2013. "Why Doing Nothing Can Revolutionize Your Company," online available: http://www.forbes.com/sites/dorieclark/2012/07/23/the-management-insight-that-could-revolutionize-your-company-do-nothing/ (last access: 10th April 2015).

Doherty, N. F., Ashurst, C., and Peppard, J. 2011. "Factors Affecting the Successful Realization of Benefits from System Development Projects: Findings from Three Case Studies," *Journal of Information Technology* (27:1), pp.1-16.

Dove, R. 2001. Response Ability: The Language, Structure, and Culture of the Agile Enterprise, New York, NY: John Wiley & Sons.

Emery, F. E. 1967. "The Next Thirty Years: Concepts, Methods and Anticipations," *Human Relations* (20), pp. 199-237.

Fichman, R. G. 2004. Real Options and IT platform Adoption: Implications for Theory and Practice. *Information Systems Research* (15:2), pp. 132-154.

Fichman, R. G., Keil, M., and Tiwana, A. 2005. "Beyond Valuation: Real Options Thinking in IT Project Management," *California Management Review* (47:2), pp. 74-100.

Galbraith, J. R. 1974. "Organization Design: An Information Processing View," *Interfaces* (4:3), pp. 28-36.

Galbraith, J. R. 2012. "The Future of Organization Design," *Journal of Organization Design* (1:1), pp. 3-6.

Guang, L., Nigussie, E., Plosila, J., and Tenhunen, H. 2014. "Positioning Antifragility for Clouds on Public Infrastructures," *Procedia Computer Science* (32), pp. 856-861.

Gigerenzer, G., and Goldstein, D. G. 1996. "Reasoning the Fast and Frugal Way: Models of Bounded Rationality," *Psychological Review* (103:4), pp. 650-669.

Harré, R. 2002. *Great scientific Experiments: Twenty Experiments that Changed our View of the World*, San Rafael, CA: Insight Editions.

Hertzum, M., Bansler, J. P., Havn, E. C., and Simonsen, J. 2012. "Pilot Implementation: Learning from Field Tests in IS Development," *Communications of the Association for Information Systems* (30:1), pp. 313-328.

Hole, K. J. 2015. "Toward Anti-fragility: A Malware-Halting Technique," *IEEE Security & Privacy* (4), p. 40-46.

Huber, G. P. (1991). "Organizational Learning: The Contributing Processes and the Literatures," *Organization Science* (2:1), pp. 88-115.

ISACA. 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*, Rolling Meadows, IL: ISACA.

Jacucci, E., Hanseth, O., and Lyytinen, K. 2006. "Introduction: Taking Complexity Seriously in IS Research," *Information Technology and People* (19:1), pp. 5-11.

Janson, M. A., and Smith, L. D. 1985. "Prototyping for Systems Development: a Critical Appraisal," *MIS Quarterly* (9:4), pp. 305-316.

Johnson, J., and Gheorghe, A. V. 2013. "Antifragility Analysis and Measurement Framework for Systems of Systems," *International Journal of Disaster Risk Science* (4:4), pp. 159-168.

Kahneman, D., and Lovallo, D. 1993. "Timid Choices and Bold Forecasts: A Cognitive Perspective on Risk Taking," *Management Science* (39:1), pp. 17-31.

Krugman, P. 2009. *The Return of Depression Economics and the Crisis of 2008*, New York, NY: W.W. Norton Company Limited.

Kephart, J. O., and Chess, D. M. 2003. "The vision of autonomic computing," *Computer* (36:1), p. 41-50.

Lee, D., Moon, J., and Kim, Y. 2007. "The Effect of Simplicity and Perceived Control on Perceived Ease of Use," in *Proceedings of the Thirteenth Americas Conference on Information Systems*, Keystone, Colorado, USA.

Lassila, K. S., and Brancheau, J. C. 1999. "Adoption and Utilization of Commercial Software Packages: Exploring Utilization Equilibria," *Journal of Management Information Systems* (16:2), pp. 63-90.

Lyytinen, K., and Hirschheim, R. 1987. "Information Systems Failures: A Survey and Classification of the Empirical Literature," *Oxford Surveys in Information Technology* (4:1), pp. 257-309.

Maeda, J. 2006. The Laws of Simplicity: Design, Technology, Business, Life, Cambridge, MA: MIT Press.

Makridakis, S., Hibon, M., and Moser, C. 1979. "Accuracy of Forecasting: An Empirical Investigation," *Journal of the Royal Statistical Society, Series A* (142:62), pp. 97-145.

Makridakis, S., and Hibon, M. 2000. "The M3-Competition: Results, Conclusions and Implications," *International Journal of Forecasting* (16:4), pp. 451-476.

Makridakis, S., Hogarth, R. M., and Gaba, A. 2009. "Forecasting and Uncertainty in the Economic and Business World," *International Journal of Forecasting* (25:4), pp. 794-812.

Makridakis, S., Hogarth, R. M., and Gaba, A. 2010. "Why Forecasts Fail. What to do Instead," *MIT Sloan Management Review* (51:2), pp. 83-90.

Makridakis, S., and Taleb, N. 2009a. "Living in a World of Low Levels of Predictability," *International Journal of Forecasting* (25:4), pp. 840-844.

Makridakis, S. and Taleb, N. 2009b. "Decision Making and Planning under Low Levels of Predictability," *International Journal of Forecasting* (25:4), pp. 716-733.

Merali, Y., and McKelvey, B. 2006. "Using Complexity Science to Effect a Paradigm Shift in Information Systems for the 21st Century," *Journal of Information Technology* (21:4), pp. 211-215.

Moss, F., Ward, L. M., and Sannita, W. G. 2004. "Stochastic Resonance and Sensory Information Processing: a Tutorial and Review of Application," *Clinical Neurophysiology* (115:2), pp. 267–81.

Müller, G., Koslowski, T. G., and Accorsi, R. 2013. "Resilience-A New Research Field in Business Information Systems?" *Business Information Systems Workshops* (160), pp. 3-14.

Nelson, R. R. 2007. "IT Project Management: Infamous Failures, Classic Mistakes, and Best Practices," *MIS Quarterly Executive* (6:7), pp. 67-78

Orlikowski, W. J., and Hofman, J. D. 1997. "An Improvisational Model for Change Management: The Case of Groupware Technologies," *Sloan Management Review* (38:2), pp. 11-22.

Overby, E., Bharadwaj, A., and Sambamurthy, V. 2006. "Enterprise Agility and the Enabling Role of Information Technology," *European Journal of Information Systems* (15:2), pp. 120-131.

Palmieri, P. A., Peterson, L. T., and Ford, E. W. 2007. "Technological Iatrogenesis: New Risks Force Heightened Management Awareness," *Journal of Healthcare Risk Management* (27:4), pp. 19-24.

Perrow, C. 1984. Normal Accidents: Living with High-Risk Technologies, New York, NY: Basic Books.

Pich, M. T., Loch, C. H., and De Meyer, A. 2002. "On Uncertainty, Ambiguity, and Complexity in Project Management," *Management Science* (48:8), pp. 1008-1023.
Pluchino, A., Rapisarda, A., and Garofalo, C. 2011a. "Efficient Promotion Strategies in Hierarchical Organizations," *Physica A: Statistical Mechanics and its Applications* (390:20), pp. 3496-3511.
Pluchino, A., Garofalo, C., Rapisarda, A., Spagano, S., and Caserta, M. 2011b. "Accidental Politicians: How Randomly Selected Legislators Can Improve Parliament Efficiency," *Physica A: Statistical Mechanics and its Applications* (390:21), pp. 3944-3954.
Popper, K. R. 1959. *The Logic of Scientific Discovery*, New York, NY: Basic Books.
Sambamurthy, V., Bharadwaj, A., and Grover, V. 2003. "Shaping Agility through Digital Options: Reconceptualizing the Role of Information Technology in Contemporary Firms," *MIS Quarterly* (27:2), pp. 237-263.
Schoemaker, P. J. 1993. "Multiple Scenario Development: Its Conceptual and Behavioral Foundation," *Strategic management journal*, (14:3), p. 193-213.
Smith, H. A., McKeen, J. D., and Staples, S. 2001. "New Developments in Practice I: Risk Management in Information Systems: Problems and Potential," *Communications of the Association for Information Systems* (7:1), Article 13.
Starfield, B. 2000. "Is US Health Really the Best in the World?" *Journal of the American Medical Association (*284:4), pp. 483-485.
Sommer, S. C., and Loch, C. H. 2004. "Selectionism and Learning in Projects with Complexity and Unforeseeable Uncertainty," *Management Science* (50:10), pp. 1334-1347.
Swanson, E. B. 2012. "The Manager's Guide to IT Innovation Waves," *MIT Sloan Management Review* (53:2), pp. 75-83.
Taleb, N. N. 2001. Fooled by Randomness: The Hidden Role of Chance in the Markets and in Life, New York: NY, Texere.
Taleb, N. N. 2010. *The Black Swan: The Impact of the Highly Improbable*, New York, NY: Random House and Penguin.
Taleb, N. N. 2012. *Anti-fragile: Things that Gain from Disorder,* New York: NY, Random House.
Taleb, N. N. 2014. Silent Risk: Lectures on Probability, Fragility, and Asymmetric Exposures, unpublished draft.
Taleb, N. N., and Douady, R. 2013. "Mathematical Definition, Mapping, and Detection of (Anti) Fragility," *Quantitative Finance* (13:11), pp. 1677-1689.
Taleb, N. N., Goldstein, D. G., and Spitznagel, M. 2009. "The Six Mistakes Executives Make in Risk Management", *Harvard Business Review* (87:10), pp. 78-81.
Taleb, N. N., and Sandis, C. 2014. "The Skin In The Game Heuristic for Protection Against Tail Events," *Review of Behavioral Economics* (1), pp. 1-21.
Teece, D. J., Pisano, G., and Shuen, A. 1997. "Dynamic Capabilities and Strategic Management," *Strategic Management Journal* (18:7), pp. 509–533.
Trier, M., and Richter, A. 2013. "I Can Simply...Theorizing Simplicity As A Design Principle And Usage Factor," in *Proceedings of the Twenty-first European Conference on Information Systems*, Utrecht, The Netherlands.
Tseitlin, A. 2013. "The Antifragile Organization: Embracing Failure to Improve Resilience and Maximize Availability," *Communications of the ACM* (56:8), pp. 40-44.
Tversky, A., and Kahneman, D. 1973. "Availability: A Heuristic for Judging Frequency and Probability," *Cognitive Psychology* (5:2), pp. 207-232.
Tversky, A., and Kahneman, D. 1974. Judgment under Uncertainty: Heuristics and Biases," *Science* (185:4157), pp. 1124-1131.
Upton, D. M., and Staats, B. R. 2008. "Radically Simple IT," *Harvard Business Review* (86:3), pp. 118-127.
Velu, C. K., Madnick, S. E., and Van Alstyne, M. W. 2013. "Centralizing Data Management with Considerations of Uncertainty and Information-Based Flexibility," *Journal of Management Information Systems* (30:3), pp. 179-212.
Volberda, H. W. 1996. "Toward the Flexible Form: How to Remain Vital in Hypercompetitive Environments," *Organization Science* (7:4), pp. 359-374.
Volberda, H. W. 1997. "Building Flexible Organizations for Fast-Moving Markets," *Long Range Planning* (30:2), pp. 169-183.

Wang, J. W., Gao, F., and Ip, W. H. 2010. "Measurement of Resilience and its Application to Enterprise Information Systems," *Enterprise Information Systems* (4:2), pp. 215-223.
Ward, A., Liker, J. K., Cristiano, J. J., and Sobek II, D. K. 1995. "The Second Toyota Paradox: How Delaying Decisions Can Make Better Cars Faster," *Sloan Management Review* (36:3), pp. 43-61.
White, L. H. 2013. "Antifragile Banking and Monetary Systems," *Cato Journal* (33:3), pp.471-484
Xue, L., Ray, G., and Gu, B. 2011. "Environmental Uncertainty and IT Infrastructure Governance: A Curvilinear Relationship," *Information Systems Research* (22:2), pp. 389-399.

Appendix 1. Table 1. Antifragile guidelines and the IT value creation processes of the IT function

	Process	Process description	Simplicity	Decentralize	Optionality	Skin in the game	Inject randomness	Reduce naïve intervention
Governing Processes	Strategic Planning	Enterprise-wide activities aimed at establishing strategic business thrusts and determining how strategic IT thrusts will support the business.						
	Monitor, Evaluate, and Assess Performance, Conformance, and Compliance	Selecting, designing, implementing, and using performance metrics. The designing, implementing, maintaining, verifying, and reporting of compliance requirements originating in regulations and law enforcements.						
Core Processes	Define Enterprise Architecture	Building and managing the blueprint for investing in computing, networking, database, object-base, and other key infrastructure technologies. Includes the establishment and management of IT infrastructure standards.						
	Deliver Solutions	Analysis of business needs for IT, conceptualizing of IT applications, and delivery of applications either through internal development, external contracting, or the integration of packaged software.						
	Provide Services	The provisioning of utilities, such as data centers, and services, such as helpdesks and desktop management, for users across the corporation.						
Enabling Processes	Manage Risks and Security	Identifying, analyzing, reducing, and monitoring IT-related risks.						
	Manage Human Capital	Identifying the know-how the IS function needs to possess, with respect to technology, business, and strategy. Acquiring, developing, and retaining IT talent.						
	Manage Quality	Defining quality standards and practices. Monitoring and reviewing internal and external performance against the defined quality standards and practices.						
	Financial Management	The structuring of service-level agreements, tracking and benchmarking the costs of IT services, and developing the business case and ROI analyses of IT infrastructure investment proposals.						
	Manage Relationships	Partnering with internal clients, external vendors, and business peers to develop a shared understanding of IS's vision and role. Managing expectations across stakeholder groups.						