SECTION ONE

Change, the Double-Edged Sword

The only constant is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be.

—Isaac Asimov

You can view change as containing many important aspects, especially when talking about evolving risk and how to manage it. These aspects include: change resulting from innovation, competitive and investor pressures, organizational realignments, geopolitical events, societal shifts, and a variety of internal and external events. In this section, I look at what's at risk as a result of change, the cause and effect of risk brought about by change, the increasingly vulnerable organization, and how value chains are created and evolve over time.

My goal in this first section is to define change and its effect on an organization's risk profile. At the root of this challenge is the reality that an organization cannot completely control the speed of change, the timing of the change, or the cascading consequences of the many risks that arise as a

result of change in our highly interconnected and interdependent global value chains. One thing is certain: with change comes risk. The challenge has always been, and will always be, to find the right balance between the "reward" that is afforded when initiating change and the "consequence" that is suffered when one poorly manages risk.

Risks created by change, and their unintended consequences, are a result of not being able to predict, forecast, or model all of the possible combinations of threats, vulnerabilities, external factors, and the many combinations of resources (labor/skills, technology and processing, physical assets, relationships) used to create value and support the value chain. The management of financial change and risk is an example of where risk is better understood, measured, modeled, managed, and highly regulated (e.g., foreign exchange, credit). To accomplish effective financial risk management the organization has to put in place strong governance, reporting, incentives, penalties, training, education, and clear expectations tolerances. However, the results of this analytical process are still subject to complex and many times unpredictable behavioral, environmental, operational, and societal influences that dramatically alter outcomes. *The primary focus of this book is on the operational view of these changes, resultant risks, and solutions to create and sustain a risk-conscious culture across the extended value chain.*

Change should not be a surprise to the organization, and neither should the risks that are associated with change. In most instances we typically find indicators, trends, signals—somewhere in the process or organization's memory (the seasoned employees with collectively hundreds of years of knowledge, experience, and intuition) - that warn us that change has occurred or is about to occur. A British psychologist, James T. Reason, came up with an accident causation model used in risk assessment referred to as the "Swiss Cheese" model. Reason hypothesizes that most accidents can be traced to one or more of four levels of failure. The theory looks at the cumulative act affect of contributory failures that have lain dormant for a long time. Simply stated, most big events don't just happen. There is typically something else that might have happened (and gone unnoticed or noticed and not reported). Something as meaningless as a small rounding error or a small amount of missing stock could be an indicator that there is a problem and that it could be much larger than anticipated. What is needed in the risk-conscious culture is the engagement of the masses to identify these symptoms and close calls and to report this upward to

management for resolution. Once surfaced, appropriate filters which validate the information and exposure must exist. Confirmed risk must be escalated immediately and responsibility for resolution assigned. How informed and prepared we are—our ability to anticipate, predict, mitigate, and respond—or how quickly we learn of and communicate the potential for negative consequences is fundamental to successful risk management. Some organizations cause change, others react to change, and some are able to avoid change altogether—until others have proven it safe to proceed. Some organizations are change agents, such as Sony, Apple, Samsung, Virgin, Toyota, Procter and Gamble, Starbucks, Wal-Mart, Intel, GE, and, of course, Google. There are different risk implications for each, and by the nature of their size or global influences, all members of their value chains are impacted by any change. Some organizations seem to be more agile than others and aggressively implement risk avoidance practices. Others practice risk mitigation and possess a resiliency characteristic that allows them to "bounce back" quickly from an adverse event. Both of these attributes, agility and resiliency, are *necessary* for successful risk management. But how does an organization identify and manage risk associated with rapid change, and how do they achieve the correct level of resiliency and agility? With so much change under way—technical, social, geographical, environmental, economic, political, and operational—how does an organization implement a sustainable and comprehensive risk program without losing sight of its main purpose— value creation and social responsibility?

To answer these questions I will use case studies to deconstruct the change and associated risk process. These historical examples of change and ineffective risk management provide us with a starting point to better understand why significant risk resulted and what lessons can be learned. Change is dynamic, often unpredictable, and necessary as it fuels innovation, progress, and growth. However, the risk associated with change is potentially at a "flash point" whereby the realization of a single risk could cascade into a mega-crisis due to the nature of our interconnected, global society and mutually interdependent value and supply chains.

CHAPTER 1

Rapid Change, *Escalating Risk*

What are you doing, Dave?

—Voice of computer HAL in *2001: A Space Odyssey*, 1968

Change—inevitable and constant. What once were vertically integrated self-contained organizations are now mass assemblers, marketers, retailers, distributors, and service organizations. They rely on others to do what they once did in a global eco-network of human, manufacturing, logistics, and finance capabilities to fulfill their primary corporate missions. Change is taking place with greater speed, efficiency, capacity, ubiquity, and anonymity. Where does it end? In the well-known film *2001: A Space Odyssey*, the oddly-named HAL (advance the name alphabetically by one letter each and see what you get) senses that astronaut Dave is about to disconnect the system, so HAL (with a sense of self-preservation) kills Dave.

The sentient computer is the ultimate disaster of progress, and may remain in the realm of science fiction. But the idea is relevant here because it shows how progress and change can turn on us and even destroy us. HAL was a supercomputer of the highest order and a miracle of "future" technology. It ultimately destroyed its creators. They enjoyed the benefits

brought about by change but failed to consider the risk. We can apply this lesson to modern-day risks that all organizations are experiencing.

The Roots of Change

Change can be imposed on the organization from a variety of sources such as clients, regulators, investors, underwriters, competitors, suppliers, and of course, Mother Nature. A change can be unexpected or the result of some unanticipated event. The latter is much riskier because the assessment, reaction, and response time is severely limited. Unfortunately, there are many instances where an overreaction or incorrect response introduced greater risk than the original event. Negative outcomes often result from individuals making quick and uninformed ("gut") decisions. The worst case of all is when the unanticipated event has already produced an overwhelming catastrophic consequence that severely limits the organization's ability to manage the risk. This occurred during the September 11, 2001, terrorist attacks; European heat wave of 2003 that killed 35,000; Bhopal gas tragedy in December 1984, where several hundred thousand people were exposed to a deadly gas; and Hurricane Katrina, where 1800 people perished and there was an estimated US$18 billion in damage. Whether anticipated or unanticipated change, the organization will need accurate and current information about the potential impacts as well as a decision-making framework to provide options and actionable advice.

The organization can initiate change that adversely impacts others, accidentally, or purposefully. Poorly coordinataed changes (all participants in the value chain) could cause consequential damages if there is a negative outcome—hence the term third-party liability.

The point here is that with every change, there is a potential upside—an opportunity to grow, expand into new markets, and/or gain market share. However, there is the potential for a downside risk when unmitigated consequences are eventually realized. To strike the balance between risk and reward requires not only accurate and timely knowledge/data but also early intervention, risk assessment, and the care and feeding of a risk-conscious culture. The process cannot begin without a thorough understanding of an organization's business priority, value chain(s), and what's at risk.

KEY LEARNING POINT

Those that do not consider risk at the onset of change, or wait until after the important "change" decisions have been made, place the organization at tremendous risk. Any change—large or small, planned or unplanned—has the potential to create material risk to the organization and its stakeholders.

For example, the organization can initiate a change such as an organizational realignment. The intent of this change might be to improve operational efficiencies. However, this change has the potential to introduce significant and material *risk* if this strategy is flawed, poorly timed, or unsuccessfully executed (I think we've all experienced at least one organizational change that resulted in less-than-desired outcomes). The key to effective and efficient risk management is a pervasive culture that knows how to identify the value-based priorities, value chain processes and resources, financial/brand/strategy impacts, and risk treatment choices and associated implementation impacts (e.g., cost, service, quality, social). I've found it helpful to look at change from the vantage points depicted in Exhibit 1.1.

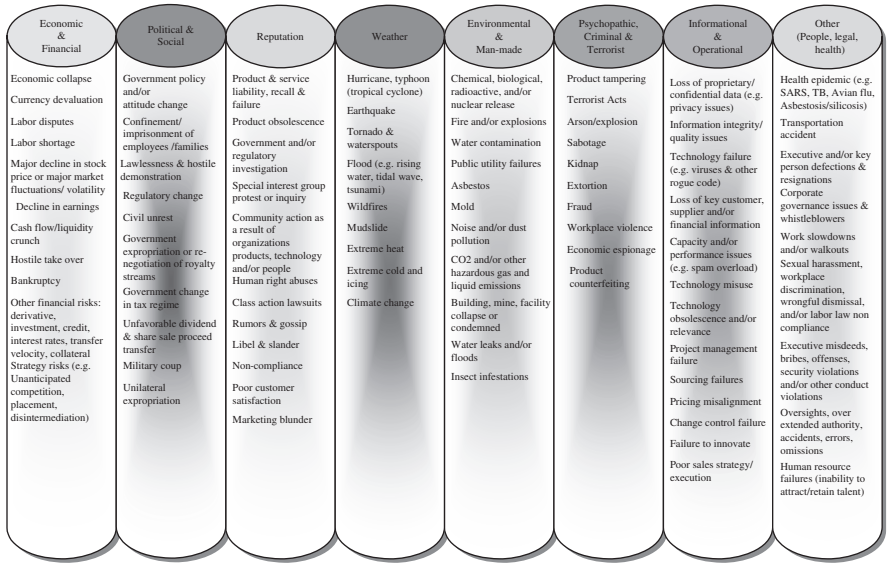

EXHIBIT 1.1 **Risk Triggers**

I begin to expose you to your journey or, if you will, your odyssey, with three case studies of change, risk, and the subsequent consequences—the long view of risk. These are not examples of the occasional low-probability, high-impact threat, such as a catastrophic terrorist incident or mega-weather-related disaster, but rather real stories about risks that organizations face daily. Risk, brought about by change—whether planned or unplanned, the consequences remain the same. The business decisions made, or not made, and the associated risk were a reflection of the organization's culture, policies, and collective experience. Unfortunately, I have found that in most instances of risk failure the final decision was based on the individual's instinct—or worse—their incentives, rather than on a disciplined risk philosophy and approach.

The goal is to deconstruct and analyze these cases to better identify/anticipate change and to harmonize risk and change processes. The first case is about a major bank that decided to decentralize its global funds transfer capabilities and, as a result, fell victim to two separate $6 million wire frauds. The change created a risk that was exploited by an insider with the assistance of at least 12 members of an organized crime ring. The second case involved a global consumer electronics company that chose to outsource the manufacturing of a critical component of their flagship product to a supplier in a poorly regulated country. A fire ensued, the outsourced manufacturer's plant was destroyed, and production of the product halted. The third case is about a bank that was seeking to improve operating margins by reducing overhead costs in the mortgage origination process. They outsourced part of the credit reporting function and as a result became a victim of an identity theft scheme perpetrated from the inside and sponsored by a notorious Nigerian organized crime ring.

Inside Looking Out: Three Case Studies of Change and *Escalating Risk*

Like most cases, it was the greed and a careless mistake on the part of the perpetrators, rather than a comprehensive system of managing risks and executing critical controls, that prevented them from walking away with

CASE 1 RAPID CHANGE: ATTRACT NEW CUSTOMERS AND STRENGTHEN RELATIONSHIPS

RISK REALIZED: $12 MILLION WIRE FRAUD AND BRAND DAMAGE

When the phone rang late on a Thursday evening, the last people that I expected to be on the other end of the line were the CIO and general auditor of the bank. In two separate incidents, $12 million had suddenly disappeared from the asset management department's balance sheets. It wasn't immediately clear whether this was an isolated breach or a large-scale attack. The treasurers of more than 1,200 major companies used the bank's PC-based treasury management system to move billions of dollars daily ($400 million was moved daily on just one PC workstation in the internal operations area). During an around-the-clock investigation, we determined that an organized crime ring, consisting of 12 people, had carefully and systematically learned about flaws in the operational processes and computerized system (no system audit trail, easily retrievable passwords on the hard drive, ability to delete or replace audit records) and, as a result, easily made off with the money. The bank was caught flat-footed, completely unaware that it was so exposed.

$12 million. However 11 out of the 12 were able to walk away with their freedom. Could this potentially disastrous situation been prevented?

Many questions had to be answered quickly (*Note:* these questions should be considered as part of your first responder/crisis plan):

- What actually happened?
- What's our risk?
- Will we have to revert to a manual payment process until we determine if there is systemic risk or until the problem is fixed?
- What's our contingent risk and liability, and who else might be impacted by this event?

- Is this happening elsewhere (i.e., on other internal or external workstations)?
- How is management going to communicate to thousands of global 500 corporations that the integrity of their cash management environment might have been compromised and at any moment they could be defrauded of hundreds of millions of dollars (if they hadn't already)? Will they trust us?
- How will we handle the barrage of questions if this goes public? Could the confidence/trust of the payments systems be undermined? Who do we need to notify immediately (customers, regulators, directors, press)?

The bank, like most other organizations, was simply overwhelmed (and perhaps unprepared) for the risks it faces every day. The warning lights were flashing: The unobserved removal of the security and audit system two weeks prior; suspicious behaviors that had occurred and never been reported, questioned, or elevated to senior management; violation logs containing evidence that someone was trying to break in, had not been reviewed; and the technical support group had been cited by the audit group for exploiting a design flaw, but this activity was never discontinued because of need to provide customer support. This situation could have been avoided if someone had noticed that a similar scheme had taken place five years earlier at Prudential Securities. This scheme was publicly reported (Equinox/Discovery Channel TV special: *Information Superhighway Robbery*) and resulted in an $8.5 million theft under very similar circumstances.

LESSONS LEARNED *In the bank's zeal to cut expenses by reducing head count, they destroyed hundreds of years of corporate memory and the inherent "risk sensitivity" of long-term, experienced employees. These employees represented the organization's sensors, the first line of defense in managing risk. Somewhere a similar exposure was reported in the press or could have been obtained through a close/confidential relationship with an industry counterpart or law enforcement and/or government agency. This was found out later in the case—the insider had been suspected of wrongdoing at another major money center bank.*

Many of the more mundane operational risks are usually not properly addressed by the development, operations, and audit teams. In this case, the "sexier" external risks, such as capturing and altering a funds transfer message in transit, was the primary focus of the risk design team. Many of the internal, operationally based risks could have easily been uncovered during the system design phase if the assessment team focused on the value chain; key processes, resources, and the broader set of people, physical and electronic vulnerabilities. Too often, published information reflecting actual security/risk crises are not identified, analyzed, and acted upon by staff responsible for assessing or managing risk. They fail to ask the questions, "Do I have the same risk exposure, is the incident relevant to my business, and could it happen here?"

CASE 2 RAPID CHANGE: IMPROVE MARGINS; OUTSOURCE MANUFACTURING

Risk Realized: Lost revenue and brand damage

"We've decided to outsource part of the manufacturing operation of our best-selling consumer electronic product," stated a product manager at a global Fortune 200 organization. Operational overhead will be reduced by 12% and delivery times shortened by a third. The supplier is located in Mexico, where labor is much less expensive, the tax systems, much more advantageous to business, and the environment is only moderately regulated. What could go wrong?

One day, a minor catastrophe occurred when there was a fire at the plant in Mexico. The facility suffered moderate damage, and that's when this company found out that its larger competitor was also sourcing parts from the same location. The supply chain was partially disrupted for a short period, but it wasn't a serious loss. However, a second fire occurred and this time it was a major fire, completely destroying the plant. The outsourced parts manufacturer's supply chain came to a screeching halt. Business interruption insurance will most likely cover the majority of the financial loss, although the carriers are challenging this assumption and asking a lot of questions about the company's risk management oversight and readiness. It appears that their flagship product will

be off the shelves for at least six months. That includes their peak selling period, the holiday season, and NFL Super Bowl. Although this product does not account for a substantial piece of the overall revenue, this Asia-based company considers not having this particular product on the shelf, right next to their competitors, a catastrophic brand embarrassment. This is a true story, but let me explain a bit more. You see, when this organization decided to move the production of this critical component to an outsourced supplier in Mexico, they failed to consider that the low-cost labor and production facility was low-cost for a reason. One of these reasons was that the fire standards didn't require the building to have sprinklers, nor did it account for the lack of adequate water supply or fire protection. To make matters worse, this company also supplied a larger competitor. When recovering their facility and operating at partial capacity, the big question became: Who will get preferential treatment? (I call this contention exposure.) Thank goodness the workers were not injured or killed; besides the horrible personal consequence for the families, think for a moment about the brand and reputation exposure if this household brand were also exposing individual employees to unsafe working conditions.

LESSONS LEARNED *Margins were squeezed as the number of competitors increased. Seeking a lower cost of goods sold, manufacturers were always on the hunt for ways to drive down labor and other production costs. All of this was predictable and obvious. However, the organization, in its quest to drive down costs, failed to apply existing property risk standards (fire) that were already in place at their facilities located in developed countries. The insurer failed to demand these standards as well. The moral of the story is that just because you decided to outsource a process in your value chain that it does not relinquish your organization's risk management responsibility. Initial risk assessment must be followed by routine and unannounced audits to validate that previously agreed risk practices are in effect. Here are several additional risk considerations. Critical risk information about the previous incidents did flow to those that could effect change. Following the first fire incident, no one performed a comprehensive risk analysis of recently discovered exposures. No steps were taken to mitigate this known and*

documented critical exposure. In addition, no one surfaced the inherent contention conflict that would result from being a less important customer of this outsourced supplier. These failures had a cascading effect that impacted current and forecasted production and many overseas jobs, lost revenue for all members of the value chain (transportation, retailers, etc.), and resulted in a major public embarrassment.

CASE 3

RAPID CHANGE: STREAMLINE MORTGAGE ORIGINATION PROCESSES AND REDUCE EXPENSES

Risk Realized: Privacy Breach, Identity Theft and Brand Damage

I received a call from our Legal Investigation unit requesting me to join them in following up on a tip provided by the FBI. It appeared that a disgruntled girlfriend was tired of her boyfriend's behavior—he was a contract employee of the bank—and decided to rat him out to the Feds. This was no ordinary boyfriend. It turned out that this individual was part of an elaborate Nigerian crime ring involved in defrauding consumers and the bank, by compromising thousands of individuals' identities.

I arrived in the office in midtown Manhattan to interview the manager of the mortgage origination business. The group consisted of 20 people who were responsible for originating millions of dollars in mortgages each month. The group had decided to keep expenses down by outsourcing one of the operations functions to a contract employee. The corporate memory and risk sensors had been lost when an experienced, long-term employee had been laid off to reduce cost. The contract employee was responsible for taking the mortgage application, which had been faxed or compiled during a phone call, and running a consolidated credit report from one of the regional credit agencies. He accessed the credit information via a PC and application provided by the credit agency. What was so ironic was that this employee had just been offered a full-time position because of exceptional performance. His fellow workers commented during the investigation process that "he worked day and night" and would come in on the weekends, just to keep pace with the work. At that moment I thought to

myself, how much volume is the group doing and what is the extent of his function? I thought he just had to push some buttons on the computer, print off a credit report, staple the report to the application, and hand it to the loan officer. Was this a sensor or warning light that something was afoul? Needless to say, when I looked closer I discovered that only 50 to 60 applications were being originated per month. However, the accounting records indicated that between 600 and 800 credit reports were being requested monthly (by the way, the bank was being billed for each of these credit inquiries, but no one noticed—another warning light?). Something did not add up. As it turned out, we discovered that this activity had been going on for approximately eight months—more than 4500 unapproved individual credit inquiries!

LESSON LEARNED

The key questions that should have been asked were:

- *Did the organization consider who and how risk would be managed when they were considering change (i.e., when reducing operational overhead via outsourcing the management of risk would no longer be performed internally)?*
- *Did they assess the risk of this change to the value chain, and did they track the flow of sensitive data through the entire value chain (i.e., from creation to destruction)?*
- *Did the organization define what constitutes sensitive data (i.e., the characteristics of the data that defined it as sensitive, e.g. regulatory requirement or privacy law)?*
- *Did the organization consider performing a threat agent assessment (i.e., a simple assessment to determine who would have the greatest opportunity—empowerment, means—to compromise the sensitive data)?*
- *Who reconciled the monthly billing against loan applications (i.e., should have surfaced the issue immediately)? In a risk-conscious culture a discrepancy like this would have immediately raised questions and been elevated to management.*

- *Why didn't a co-worker or manager notice, report, and question why a temporary employee was working hundreds of paid overtime hours— including weekends and evenings when the operation was closed?*

Management must create and nurture a risk-sensitive culture as well as train their employees and others in the field, on how to detect risk warning signs occurring in every critical process. Often, the observation of an unusual occurrence should be all that is needed to set off the risk sensors.

Guidelines for rapid report and escalation must be established. It is important that employees are incentivized and feel empowered to raise the warning flags. Management must be responsible and accountable to address and resolve all risk issues raised.

These are some of the many examples of risk assessment that could have easily helped to avoid significant brand damage, legal exposure, and financial loss. Why wasn't risk addressed early in the change process?

What's Changed and What Risk Has Been Brought About by Change?

These cases reflect that the identification of change is often elusive and difficult to spot. Like the old adage about the frog and boiling water—that is, throw the frog in boiling water and it will jump out, place the frog in the pan with heat increasing gradually and the frog might not realize the change, or its impact, until it's too late (of course, I don't advocate this behavior—it is merely used as a representation). You might not be aware of change or its impact on the processes and resources that support your value chain.

Processes change as they become automated; are improved for efficiency; are impacted by policy change; are adapted to organizational realignment; are migrated to outsourced partners; are transitioned outside of domestic borders; or are changed for multinational implementation. For example, the sourcing and importing of materials outside of domestic borders now is under close post-9/11 security scrutiny and new customs regulations apply for those seeking to be compliant with Authorized Economic Operators or U.S. Customs-Trade Partnership Against Terrorism (C-TPAT) standards (a voluntary supply chain security program led by U.S. Customs and Border Protection). This is a major change/risk to

many organizations' value chains since it requires additional security diligence and, if not managed properly, will result in significant shipment delays.

Movement to offshore suppliers further complicates how work is done and, more to the point, how risks grow as well. Intellectual property theft, geographies more prone to natural hazards, availability of localized skilled labor, inferior product quality standards, and other risks increase exponentially when the value chain transitions from a vertically integrated, self-contained set of processes to a geographically disbursed linked set of relationships. This interdependent virtual eco-network consists of hundreds or thousands of public and private stakeholders. In most instances, these relationships appear to be strong and well defined. The reality is that when the perceived value of the relationship (we are all in this together) begins to diminish between, let's say, a supplier and the organization, these relationships dissolve and new ones are formed. New suppliers arrive on the scene and compete for the business. If the new vendors improve profitability or the return on investment/assets then the switch is made—or better stated—change occurs and risk is created. Unfortunately, pressures to change to more reliable partners, and the need to keep products flowing, often result in shortcuts being taken.

A few examples of the risks that arise as a result of this change are: 1) not properly deactivating physical or computer information access, or debriefing the former supplier, 2) failure to assess and integrate the new supplier's processes and technology, and 3) inheriting contingent supplier risk. In many instances the supplier relationship is not as important as having access to a pool of suppliers that can provide the raw material. As one senior executive at a high tech company recently told me "We don't really care about most suppliers, what we care about is the supply of the raw material. If our primary supplier fails, then we'll just find another. We only care when enough of the suppliers fail to cause a change in material price." The point here is to remember that you typically only have one chance and that inconsistent or unpredictable performance levels will be tolerated less and less as globalization continues to take hold. Although you might perceive that your organization has an unbreakable relationship with your customer, in today's global marketplace failure will not be tolerated, and there is always a competitor anxiously waiting somewhere—in India, Brazil, the United States, Vietnam, Russia, China, and elsewhere—to displace you.

One final point to remember about change: when your organization experiences change, you want to make sure the *improvement* is still viewed positively when long-term impacts are factored in. This requires consideration of the cost, service, quality, and social implications when implementing and supporting risk solutions. Also, the behavioral impact cannot, and should not, be underestimated when implementing risk solutions. To determine the long-term effectiveness of the control, ask yourself, "How likely will this control be accepted and adapted into the operational workflow?" Talk to your peers, public- and private-sector experts around the globe and within your industry, your risk-conscious network, and others who have experienced similar change. What you seek at this point is risk knowledge and a consciousness of what is at risk and how your particular way of creating value, possibly supported via a complex value chain, creates risk and risk resolution challenges. All too often, the net result of change (improvement less risk impact), viewed over the longer term, is just the opposite of what you desire: lower profits, loss of quality, and increased risk.

The past few decades have been nothing short of an economic, social, and technological revolution. Change has occurred on a massive scale, and it is this change that has allowed many to achieve prosperity and growth beyond anyone's expectations. However, the upside risk (sometimes referred to in the insurance industry as *variable risk*) experienced by so many may not have forced these organizations to assess just what type of vulnerability or downside risk was being created. Faster, better, cheaper—the recurring and continuously accelerating trend fueled by the increasing number of emerging economies that are participating in the global market. It is no wonder why the management of risk, what many perceive as a potential obstacle to achieving growth, has not been widely implemented as part of this "change" process. The result is evident by the recent rash of product failure (both design and manufacturing), environmental pollution, child labor issues, subprime lending crises, communication failures, and IT breaches. The change process is moving much too fast for organizations to try and retrofit risk management solutions. As a result, the vulnerability gap continues to increase as value chains grow and become more interdependent. Those that lack the risk-conscious culture and have failed to integrate risk activities into the change process will be more exposed than ever.

SIDEBAR

Change has to be managed carefully to ensure that the organization gets the return on change it seeks. The ultimate goal of any business is to quickly produce the highest-quality product at the least cost. This has sometimes been referred to as the "Fast, Good, Cheap" production paradigm. However, history has revealed that achieving and sustaining all three attributes is impossible. If it's fast and cheap, it can't be good; good and cheap, it can't be fast; and fast and good, it can't be cheap.

It is fair to say that the "unbalanced triangle," representing the three attributes—fast, good, and cheap—all too often excludes considerations of *risk*. If you expand the triangle into a pyramid, recognizing that the fourth point is often invisible and resides behind the three front points, you can begin to appreciate the real nature of risk. It is often invisible. The triangle is two-dimensional, whereas the pyramid adds the third dimension to the picture. (See Exhibit 1.2.) Once this fourth point is added, you are better able to quantify the concept of fast, good, and cheap in terms of the risks involved. The more you are able to achieve these three attributes, the stronger the risk element is likely to be.

1. Many leaders appreciate the advantages of improved technology, development of global markets, and the availability of low-cost labor and materials from other countries. At the same time, they have not confronted the corresponding vulnerabilities that this new environment creates, such as how to trust your reputation and business that you used to own to an unknown, one where the background of the workforce or supplier cannot be validated

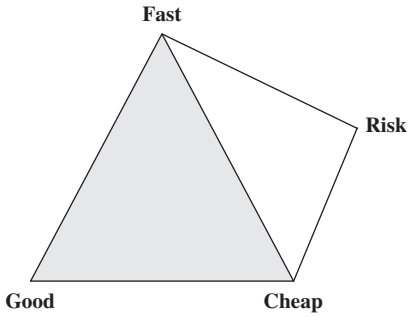

EXHIBIT 1.2 **Unbalanced Triangle.**

or actively monitored or one that operates in a part of the world with poor public infrastructure, political instability, or limited labor and environmental regulation.

2. Management typically lacks an unobstructed view (i.e., clear end-to-end "line of sight") of their product/service value chain. Here are a few questions to determine if your organization has a clear line of sight. What problems is the value chain solving? Where does the sourcing of our product/service begin (field, forest, farm, mine)? What are all of the processes in the end-to-end value chain that must be performed to create value? What resources are relied upon to create value—from the beginning of the process to the end (e.g., from the farm to the customer's mouth)? Is there a clear line of sight of all resources and associated risks? (*Note:* resources can be grouped into four categories: people/skills, technology and processing, physical assets, and relationships). Someone upstream or downstream in the supply chain management has *assumed* that someone else is adequately managing the risk.
3. Risk itself is a moving and evolving target. In our brave new world it is impossible to predict what events will occur or what risk will be realized. There is an opportunity to finance risk, via transfer products (e.g., insurance or catastrophe bonds), when there is a degree of certainty or predictability. However, risk financing is limited to that which can be clearly defined and calculated. For example, insurance/reinsurance carriers in the property market cannot create capacity in the market without a clear definition of a peril and knowing when the loss starts and stops. Therefore, the burden is on the organization and its stakeholders to mitigate (or knowingly accept) the ever-growing risk to labor, technology, processing, physical assets, and/or relationships. However, Wall Street and Main Street do not like, and will not tolerate, surprises or excessive volatility. My experience and battle scars have taught me that rapid change without a value-aligned, well-defined, disciplined, measured, operationally integrated, holistic process for managing risks and establishing a risk-conscious culture is a recipe for eventual disaster. Those without the "plan" typically find themselves trying to support inconsistent and duplicate risk initiatives. Most just need a place to start.

Also not considered by many organizations was, and still is, what I refer to as the long view—the long-term implications and subsequent impacts of the failure to effectively and efficiently manage risk. The short view typically reveals that all is fine and the risk of change was handled properly. The long-term view requires the organization to have the foresight to understand what risks are created by their actions. Unfortunately, the consequence of the risk that is realized later on is usually more significant since multiple value chains have been integrated and more organizations participate. Here are a few examples:

- Large money center banks, rapid loan portfolio expansion, and the subsequent multibillion dollar loan defaults by organizations doing business in lesser developed countries/LDCs (late 1970s/early 1980s).
- Overexpansion of the employment ranks by global financial institutions in the mid-1980s driven by technological change and deregulation of financial markets ("big bang" era). Then came the subsequent massive layoffs and business shutdowns.
- The proliferation of the e-business model and Internet businesses during the "dot-com" era (1990s) and the subsequent failed Internet start-ups (although there were some successes, such as Amazon and Yahoo) and massive financial market volatility. The impact extended to many secondary businesses such as advertising, recruiting, housing, and financial organizations.
- The rush to outsource key functions to create a lower-cost, geographically-distributed value chain causing enormous product quality and environmental issues. We are now beginning to experience rising labor costs in many of the major outsourcing countries such as India, and as a result there have been a few cases of reversing the process (in-sourcing[1]).
- The acceptance of subprime lending and the rapid creation, and subsequent failure, of a niche financial industry.

Some of those that have profited in the short term from the upside, the so-called rainmakers have reaped the rewards and moved on before the downside becomes reality. The masses are usually left to suffer the long-term impacts, such as loss of their employment/investments, buying power or worst case—their quality of life and/or health.

Many will argue that these so-called rainmakers were a necessary evil and that they were needed to spur economic prosperity and social growth. That's a matter of opinion and one's perspective, I guess, but it is my belief that the long-term ramifications of many of these risk-consciousless changes have not yet been realized.

KEY LEARNING POINT

Bottom line, the risk profile of the value chain is ever changing and therefore requires constant review, testing and a commitment to improvement. Everyone has a responsibility to participate and contribute in the organizations risk consciousness. The risk discussion should be deeply embedded, *early*, in the business change discussion. In the end, risk taking is essential part of the business.

As the chairman of a Fortune 500 company, points out: "Risk is like heat—too much and you get burned, too little and you freeze." Make no mistake, risk taking is essential.

ENDNOTE

1. Don Clark and Vibhuti Agarwa, "Some in Silicon Valley Begin to Sour on India," *Wall Street Journal*, Tuesday, July 3, 2007.