Chapter 7
Systemic and Systematic Risk

> *A very small cause which escapes our notice determines a considerable effect that we cannot fail to see, and then we say that the effect is due to chance.*
>
> —Henri Poincare

Abstract The main goal of any risk management practice is to be able to insure an acceptable level of predictability in order to gain a lead-time to mitigate a possible risk. However, until new risk management approaches are employed to fill the gap between the known and unknown, most crises will continue to come as a surprise. Risk is latent until an external event or an internal process will reveal its existence. Predictive analysis is an indispensable tool that can help decision makers preemptively test all possible or even some perceived impossible operational scenarios before a risk transforms into crisis or disaster. To be prepared is a better position than to discover the risk too late for business continuity or disaster recovery measures. In this way, predictive emulation becomes necessary for appropriate risk mitigation.

Introduction

In the past, companies have tried to manage risks by focusing on potential threats outside the organization: competitors, shifts in the strategic landscape, natural disasters, or geopolitical events. They are generally less adept at detecting internal vulnerabilities that make breakdowns not just likely but in many cases, inevitable. Vulnerabilities enter organizations and other human-designed systems, as they inevitably grow more complex. Indeed, some systems are so complex that they defy a thorough understanding.

N. Abu el Ata, R. Schmandt, *The Tyranny of Uncertainty*,
DOI 10.1007/978-3-662-49104-1_7

Examples of Risk Management Failures

Ericsson

In March 2000, a fire struck a semiconductor plant in New Mexico, leaving Ericsson Inc. short of millions of chips that the Swedish telecom giant was counting on to launch a new mobile phone product. As a result, Ericsson was ultimately driven from the market while its rival Nokia Corp. flourished. Ericsson had failed to recognize the New Mexico plant as a bottleneck in a complex, interconnected global supply chain.

Barings Bank

In February 1995, Barings Bank, Britain's oldest merchant bank (it had financed the Napoleonic wars, the Louisiana Purchase, and the Erie Canal) went from strength and prestige to bankruptcy over the course of days. The failure was caused by the actions of a single trader—Nick Leeson—who was based in a small office in Singapore. Soon after Leeson's appointment as general manager of Barings Securities Singapore, he used a secret account to hide losses he sustained engaging in the unauthorized trading of futures and options. The complexity of the Barings systems enabled Leeson to fool others into thinking that he was making money when in fact he was losing millions. But after the January 1995 Kobe, Japan, earthquake had rocked the Asian financial markets, Leeson's accumulated losses—some $1.4 billion—became too enormous to hide, eventually leading to Barings' collapse.

Malaysia Airlines

In August 2006, a defective software program aboard a Malaysia Airlines jetliner flying from Perth, Australia, to Kuala Lumpur, Malaysia, supplied incorrect data about the aircraft's speed and acceleration. This confused the flight computers, which sent the Boeing 777 on a 3000-ft roller-coaster ride. With more than five million lines of code, aircraft software programs have become too large and complex to be tested thoroughly and are fielded without any guarantee that they will always work.

Boston Scientific Corp.

Legal codes and agreements have also become increasingly complicated, often resulting in loopholes that others can exploit. In the spring of 2006, Boston Scientific Corp., a medical device manufacturer, acquired its rival Guidant Corp., outbidding Johnson & Johnson in the process. Earlier, in order to gain rapid antitrust approval, Boston Scientific and J&J had both signed deals with pharmaceutical giant Abbott Laboratories in anticipation of the Guidant acquisition. J&J was first to strike a conditional licensing deal with Abbott, but the agreement failed to include a non-compete clause so Abbott was then able to help Boston Scientific—which it happily did. After Boston Scientific outbid J&J, it sold Guidant's lucrative stent business to Abbott to alleviate regulators' monopoly concerns. Thus, by exploiting a weakness in a complex legal agreement, Abbott was able to claim the best part of Guidant's business in return for its assistance of Boston Scientific.

Comair

Time is often an enemy not only because of obsolescence and increasing wear and tear but also, ironically, because of the human ability to adapt to untenable situations and resist change. Consider, for example, the information technology system of the U.S. airlines Comair Inc. In 2004, after its acquisition by Delta Air Lines Inc., Comair was forced to shut its business for several days because of an overloaded legacy crew-management system. The result: 3900 cancelled or delayed flights, nearly 200,000 stranded passengers and a loss of $20 million in operating costs and lost revenue. Not only had the system exceeded its capacity (Comair's business had been growing healthily for years), it also suffered from the addition of layers and layers of applications. Yet Comair's IT department was reluctant to upgrade the system, as users had grown used to it. To make matters worse, Comair's acquisition by Delta created additional complications: tight constraints on capital expenditures and friction between Comair employees and their new owners had eroded the IT department's commitment. This combination of technological and organizational complexities created the *"perfect storm"* for an internal meltdown.

Unknowns Are Often the Greatest Contributors of Risk

Obviously the main goal of any risk management practice is to be able to insure an acceptable level of predictability in order to gain a lead-time to mitigate a possible risk. However, reoccurring crises of various origins expose many of the problems of risk management practices today. None of the popularized risk management practices take into consideration the impact of dynamic complexity on predictability. As

a result, many cases of risk reporting represent only part of the risk experience. Until new risk management approaches are employed to fill the gap, most crises will continue to come as a surprise, especially as they relate to the following examples.

Financial Crisis

Many studies have tried to correlate market events to financial crisis, while others point to the cyclic nature of financial environments and a third category perform post-crisis analysis in an attempt to identify the patterns that lead to crisis. Most of studies rely on the use of past data (big data and analytics) to derive trends and formulation that correspond in many cases to a partial understanding of the dynamics involved. Such dynamics produces the kind of *"unknown unknown"* Nassim Taleb[1] was talking about that prevent sound prediction and full control.

Pandemic

An epidemic is an outbreak of a contractible disease that spreads through a human population. A pandemic is an epidemic whose spread is global. There have been many epidemics throughout history, such as the Black Death. In the last hundred years, significant pandemics include:

- The 1918 Spanish flu pandemic, killing an estimated 50 million people worldwide;
- The 1957–1958 Asian flu pandemic, which killed an estimated one million people;
- The 1968–1969 Hong Kong water flu pandemic;
- The 2002–2003 SARS pandemic;
- The AIDS pandemic, beginning in 1959.
- The H1N1 Influenza (Swine Flu) Pandemic 2009–2010.

Other diseases that spread more slowly, but are still considered to be global health emergencies by the WHO, include:

- XDR TB, a strain of tuberculosis that is extensively resistant to drug treatments;
- Malaria, which kills an estimated 1.6 million people each year;
- Ebola virus disease, which has claimed hundreds of victims in Africa in several outbreaks.

[1] Taleb, Nassim Nicholas. *Fooled by Randomness*. Random House Trade Paperbacks; 2 updated editions. 23 August 2005. Print. ISBN-13: 978-0812975215.

Despite an improved ability to identify historic patterns of risk, it's the mutation and transformation factors in many pandemic cases that create new risks corresponding to new patterns of disease or transmission that make containment difficult.

Software Risk and Adaptability

Information technology (IT) disasters can be damaging, disruptive, and downright dangerous. In the age of social media individuals can now voice their criticisms online. As a result, technical failures can cause lasting reputational damage and create a trust crisis capable of impacting large numbers of customers and shareholders.

1. Obamacare's website ran into major problems when the flagship of the president's public health initiative failed to work on launch in October 2014. U.S. citizens seeking health insurance were denied access to the website and had to resort to phone lines and postal services. A lack of testing was flagged as the key reason behind the failure and healthcare officials were left looking incompetent and badly prepared. The same kind of problems happened in deploying the new automated French Tax system in 2006.
2. Sabre travel booking system: the global travel industry was thrown into chaos during the peak of the school holiday season when Sabre's worldwide reservation system—deployed by over 300 airlines—went down, causing cancellations and delays for hundreds of thousands of passengers, despite the system being offline for less than three hours.
3. NatWest system failure: the bank ran into problems when system glitches caused chaos, denying ATM, chip and pin, and internet banking facilities to customers, who took to Twitter to criticize the company and its handling of the problem. RBS also suffered a similar problem, which has led to some experts talking about the underinvestment in banking IT.
4. NHS: a computer meltdown at Scotland's biggest health board led to 500 operations and appointments being postponed. A major IT glitch with NHS Greater Glasgow and Clyde's servers meant doctors and nurses were unable to access vital patient information. Luckily no patient lives were endangered during the system failure.
5. Walmart's electronic bargains: shoppers logging on to Walmart's website thought they'd bagged a bargain when they managed to buy computer monitors and projectors—valued at $500—for as little as $8.99. The retailer blamed IT glitches causing data discrepancies. Walmart refused to honor these bargain deals, cancelling customer purchases to the relief of its shareholders, but to the outrage of customers who then vented their fury on social media.
6. Bank of England hardware failure: UK investors were left in the dark when the BofE had to resort to using backup systems due to a technical failure. The

failover meant the BofE was unable to make its quantitative easing announcement, based on which gilts it would purchase, causing disruption, and confusion for the markets.

7. California's payroll failures: The Californian state government is suing SAP over a failure to adequately develop and test a botched upgrade of its payroll system, causing problems for many of its 240,000 workforce. SAP has denied responsibility, blaming the Californian controllers' office for not properly managing the upgrade. The payroll system was decades old, so an upgrade was always going to be problematic.

Conclusion

Risk is latent until an external event or an internal process will reveal its existence. Predictive analysis is indispensable tool that can help decision makers preemptively test all possible or even some perceived impossible operational scenarios before a risk transforms into crisis or disaster. To be prepared is a better position than to discover the risk too late for business continuity or disaster recovery measures. In this way, predictive emulation becomes necessary for appropriate risk mitigation.