Module 1: An Introduction to Risk Management

Table of Contents

Case Study: The Risks of E-exposures

Electronic risk, or e-risk, comes in many forms. Like any property, computers are vulnerable to theft and employee damage (accidental or malicious). Certain components are susceptible to harm from magnetic or electrical disturbance or extremes of temperature and humidity. More important than replaceable hardware or software is the data they store; theft of proprietary information costs companies billions of dollars. Most data theft is perpetrated by employees, but "netspionage"—electronic espionage by rival companies—is on the rise.

Companies that use the Internet commercially—who create and post content or sell services or merchandise—must follow the laws and regulations that traditional businesses do and are exposed to the same risks. An online newsletter or e-zine can be sued for libel, defamation, invasion of privacy, or misappropriation (e.g., reproducing a photograph without permission) under the same laws that apply to a print newspaper. Web site owners and companies conducting business over the Internet have three major exposures to protect: intellectual property (copyrights, patents, trade secrets); security (against viruses and hackers); and business continuity (in case of system crashes).

All of these losses are covered by insurance, right? Wrong. Some coverage is provided through commercial property and liability policies, but traditional insurance policies were not designed to include e-risks. In fact, standard policies specifically exclude digital risks (or provide minimal coverage). Commercial property policies cover physical damage to *tangible* assets—and computer data, software, programs, and networks are generally not counted as tangible property. (U.S. courts are still debating the issue.)

This coverage gap can be bridged either by buying a rider or supplemental coverage to the traditional policies or by purchasing special e-risk or e-commerce coverage. E-risk property policies cover damages to the insured's computer system or Web site, including lost income because of a computer crash. An increasing number of insurers are offering e-commerce liability policies that offer protection in case the insured is sued for spreading a computer virus, infringing on property or intellectual rights, invading privacy, and so forth.

Cybercrime is just one of the e-risk-related challenges facing today's risk managers. They are preparing for it as the world evolves faster around cyberspace, evidenced by record-breaking online sales during the 2005 Christmas season.

Sources: Harry Croydon, “Making Sense of Cyber-Exposures,”National Underwriter, Property & Casualty/Risk & Benefits Management Edition, 17 June 2002; Joanne Wojcik, “Insurers Cut E-Risks from Policies,” Business Insurance, 10 September 2001; Various media resources at the end of 2005 such as Wall Street Journal and local newspapers.

Case Study: Risks in the New Millennium

While man-made and natural disasters are the stamps of this decade, another type of man-made disaster marks this period. [3]Innovative financial products without appropriate underwriting and risk management coupled with greed and lack of corporate controls brought us to the credit crisis of 2007 and 2008 and the deepest recession in a generation. The capital market has become an important player in the area of risk management with creative new financial instruments, such as Catastrophe Bonds and securitized instruments. However, the creativity and innovation also introduced new risky instruments, such as credit default swaps and mortgage-backed securities. Lack of careful underwriting of mortgages coupled with lack of understanding of the new creative “insurance” default swaps instruments and the resulting instability of the two largest remaining bond insurers are at the heart of the current credit crisis.

As such, within only one decade we see the escalation in new risk exposures at an accelerated rate. This decade can be named “the decade of extreme risks with inadequate risk management.” The late 1990s saw extreme risks with the stock market bubble without concrete financial theory. This was followed by the worst terrorist attack in a magnitude not experienced before on U.S. soil. The corporate corruption at extreme levels in corporations such as Enron just deepened the sense of extreme risks. The natural disasters of Katrina, Rita, and Wilma added to the extreme risks and were exacerbated by extraordinary mismanagement. Today, the extreme risks of mismanaged innovations in the financial markets combined with greed are stretching the field of risk management to new levels of governmental and private controls.

However, did the myopic concentration on terrorism risk derail the holistic view of risk management and preparedness? The aftermath of Katrina is a testimonial to the lack of risk management. The increase of awareness and usage of enterprise risk management (ERM) post–September 11 failed to encompass the already well-known risks of high-category hurricanes on the sustainability of New Orleans levies. The newly created holistic Homeland Security agency, which houses FEMA, not only did not initiate steps to avoid the disaster, it also did not take the appropriate steps to reduce the suffering of those afflicted once the risk materialized. This outcome also points to the importance of having a committed stakeholder who is vested in the outcome and cares to lower and mitigate the risk. Since the insurance industry did not own the risk of flood, there was a gap in the risk management. The focus on terrorism risk could be regarded as a contributing factor to the neglect of the natural disasters risk in New Orleans. The ground was fertile for mishandling the extreme hurricane catastrophes. Therefore, from such a viewpoint, it can be argued that

September 11 derailed our comprehensive national risk management and contributed indirectly to the worsening of the effects of Hurricane Katrina.

Furthermore, in an era of financial technology and creation of innovative modeling for predicting the most infrequent catastrophes, the innovation and growth in human capacity is at the root of the current credit crisis. While the innovation allows firms such as Risk Management Solutions (RMS) and AIR Worldwide to provide models [4] that predict potential man-made and natural catastrophes, financial technology also advanced the creation of financial instruments, such as credit default derivatives and mortgage-backed securities. The creation of the products provided “black boxes” understood by few and without appropriate risk management. Engineers, mathematicians, and quantitatively talented people moved from the low-paying jobs in their respective fields into Wall Street. They used their skills to create models and new products but lacked the business acumen and the required safety net understanding to ensure product sustenance. Management of large financial institutions globally enjoyed the new creativity and endorsed the adoption of the new products without clear understanding of their potential impact or just because of greed. This lack of risk management is at the heart of the credit crisis of 2008. No wonder the credit rating organizations are now adding ERM scores to their ratings of companies.

The following quote is a key to today’s risk management discipline: “Risk management has been a significant part of the insurance industry…, but in recent times it has developed a wider currency as an emerging management philosophy across the globe…. The challenge facing the risk management practitioner of the twenty-first century is not just breaking free of the mantra that risk management is all about insurance, and if we have insurance, then we have managed our risks, but rather being accepted as a provider of advice and service to the risk makers and the risk takers at all levels within the enterprise. It is the risk makers and the risk takers who must be the owners of risk and accountable for its effective management.” [5]

Case Study: Is Airport Security Worth It to You?

Following the September 11, 2001, terrorist attacks, the Federal Aviation Administration (now the Transportation Security Administration [TSA] under the U.S. Department of Homeland Security [DHS]) wrestled with a large question: how could a dozen or more hijackers armed with knives slip through security checkpoints at two major airports? Sadly, it wasn't hard. Lawmakers and security experts had long complained about lax safety measures at airports, citing several studies over the years that had documented serious security lapses. "I think a major terrorist incident was bound to happen," Paul Bracken, a Yale University professor who teaches national security issues and international business, told Wired magazine a day after the attacks. "I think this incident exposed airport security for what any frequent traveler knows it is—a complete joke. It's effective in stopping people who may have a cigarette lighter or a metal belt buckle, but against people who want to hijack four planes simultaneously, it is a failure."

Two days after the attacks, air space was reopened under extremely tight security measures, including placing armed security guards on flights; ending curbside check-in; banning sharp objects (at first, even tweezers, nail clippers, and eyelash curlers were confiscated); restricting boarding areas to ticket-holding passengers; and conducting extensive searches of carry-on bags.

In the years since the 2001 terrorist attacks, U.S. airport security procedures have undergone many changes, often in response to current events and national terrorism threat levels. Beginning in December 2005, the Transportation Security Administration (TSA) refocused its efforts to detect suspicious persons, items, and activities. The new measures called for increased random passenger screenings. They lifted restrictions on certain carry-on items. Overall, the changes were viewed as a relaxation of the extremely strict protocols that had been in place subsequent to the events of 9/11.

The TSA had to revise its airline security policy yet again shortly after the December 2005 adjustments. On August 10, 2006, British police apprehended over twenty suspects implicated in a plot to detonate liquid-based explosives on flights originating from the United Kingdom bound for several major U.S. cities. Following news of this aborted plot, the U.S. Terror Alert Level soared to red (denoting a severe threat level). As a result, the TSA quickly barred passengers from carrying on most liquids and other potentially explosives-concealing compounds to flights in U.S. airports. Beverages, gels, lotions, toothpastes, and semisolid cosmetics (such as lipstick) were thus expressly forbidden.

Less-burdensome modifications were made to the list of TSA-prohibited items not long after publication of the initial requirements. Nevertheless, compliance remains a controversial issue among elected officials and the public, who contend that the many changes are difficult to keep up with. Many contended that the changes represented too great a tradeoff of comfort or convenience for the illusion of safety. To many citizens, though, the 2001 terrorist plot served as a wake-up call, reminding a nation quietly settling into a state of complacency of the need for continued vigilance. Regardless of the merits of these viewpoints, air travel security will no doubt remain a

hot topic in the years ahead as the economic, financial, regulatory, and sociological issues become increasingly complex.

Questions for Discussion

1. Discuss whether the government has the right to impose great cost to many in terms of lost time in using air travel, inconvenience, and affronts to some people's privacy to protect a few individuals.

2.Do you see any morale or moral hazards associated with the homeland security monitoring and actively searching people and doing preflight background checks on individuals prior to boarding?

3.Discuss the issue of personal freedom versus national security as it relates to this case.

Sources: Tsar's Press release

At http://www.tsa.gov/public/display?theme=44&content=090005198018c27e. For more information regarding TSA, visit our Web site at http://www.TSA.gov; Dave Linkups, "Airports Vulnerable Despite Higher Level of Security,"Business Insurance, 6 May 2002; "U.S. Flyers Still at Risk,"National Underwriter Property & Casualty/Risk & Benefits Management Edition, 1 April 2002; Stephen Power, "Background Checks Await Fliers," The Wall Street Journal, 7 June 2002. For media sources related to 2006 terrorist
plot,seehttp://en.wikipedia.org/wiki/2006_transatlantic_aircraft_plot#References