

Identifying and Managing Risk in the Global Corporate Environment

Mark Kleinsteuber
Life Safety Department
Industrial Design and Construction

Abstract

As today's global society grows, so too grow the risks to our corporate environments. Identifying and managing these risks is becoming a greater challenge in the face of economic globalism. Risks facing corporations today include environmental liability, political and product liability, business interruption, employee protection, patent protection, and others. These risks present challenges to the overall strategic success of the corporation. This paper will highlight current risk management strategies and the advanced systems capable of supporting those strategies, with the purpose of helping managers identify successful and cost-effective risk management strategies specific to their circumstances.

Introduction

Defining risks, particularly in corporate circles, frequently brings to mind regulatory agencies, codes and standards, and many other factors related to the limitation of physical harm and financial impacts to the corporation. Some of these regulatory standards include: General Duty Clause, OSH Act Section 654, Process Safety Management Standard, 29CFR 1910.119, and the Hazard Communication Standard, 29 CFR 1910.1200. These and other regulations relative to risk management and the inherent protection of personnel and prevention of financial loss are the product of years of practical application, trial and error, and carefully calculated analyses. All too often, typical risk assessment and emergency preparedness meetings with the local authority having jurisdiction tend to have one-way communication channels – the authority informing the corporation of their requirements and expectations. The corporate risk managers then go back and determine what means and methods they will utilize to meet the requirements of the authorities. While valid concerns that are indeed addressed by risk professionals, these regulatory impacts tend to be the drivers of tangible risk management strategies rather than an overall risk management plan, addressing only the minimization of loss while ignoring the maximization of stakeholder¹ interest. The consequences of poor communication to stakeholders of the risk management plan can result in far greater losses to the corporation than those directly impacting the balance sheet.

Stakeholder Interests versus Compound Interest

An environmental release affects corporate coffers not only through regulatory fines and possible process shutdown resulting in lost revenues, but could also have an impact on the health and safety of the community. This might well affect the corporation's social impact in the community, thereby limiting public support of future expansion plans of the facility and, at worst, destroying the confidence of the community and driving the corporation out. The impact on all stakeholders has a deeper effect than just the monetary impact to the corporation. Therefore, in addition to the regulatory requirements imposed, corporate risk managers need to be very cognizant of the overall impact of the risks being evaluated, as well as the methods necessary to diminish these risks. Risk managers should consider multiple contributory events and consequences when evaluating and analyzing the risks to their corporation. Their plans should be assertively and effectively communicated to all stakeholders.

Another example of minimizing risk management to purely financial consequences is the relative newcomer in the risk assessment arena, which is interdependence on the Internet and the consequences of a significant Internet outage. With the globalization of our economies and the consequent interdependence of those economies, the Internet has become a most effective tool for communicating and transacting. Electronic sabotage has become a very real threat to the effective operation of our corporations. A very effective method of protecting the corporate Intranet, Extranet, and Internet, as well as computing hardware integrity is the utilization of recognition systems. Currently, the most widely accepted method of security for computer networks is ironically one of the most easily defeated – the

¹ Stakeholder, in this context, is defined as all of those impacted by the effective management of risk, including employees, customers, suppliers, investors, regulators and the community.

password. Recognition systems -- iris, retinal, facial and others are very effective deterrents, as the majority of these “technical signatures” cannot be replicated. With the recent technological advances in these systems, and the reduced costs, recognition systems are proving to be very effective in controlling “virtual risks.” However, the financial havoc wreaked on an organization by a single hacker or the damage inflicted by a terrorist’s attack on our communications infrastructure can have catastrophic impacts on a corporation’s ability to recover. While most corporations are currently identifying and minimizing business interruption and its monetary impact, the hidden long-term effect on the corporation is lost confidence from those stakeholders left out of the corporation’s communication of its risk management and recovery plans.

Business interruption is, in many cases, the most costly effect of financial hardship stemming from risk scenarios. A primary example is the number of business closings and bankruptcies that have occurred and will continue to occur as a consequence of the September 11 attacks. In an economy driven by short-term earnings reports, many of our corporations are sacrificing reliable financial contingencies for unstable fiscal policies. As part of a resilient risk management plan, corporations should be prepared, with reasonable certainty and prudent evaluation of risks, to have sufficient, dependable resources available for recovery from business interruption. Additionally, the planned implementation of these resources should be communicated with confidence to the corporation’s stakeholders.

Security and Safety

Security and safety for the corporation’s facility and its personnel have taken on new meaning in the past several years and this aspect of risk management has become of paramount importance in the past several months. Physical security protection has long been an important consideration, both from an asset protection standpoint, as well as from an employee protection standpoint. Most corporate risk managers are highly insightful to the traditional methods of managing security threats, such as special lighting, perimeter and interior intrusion detection, access control, and video surveillance. New technologies are emerging to address new risks. Mail scanning and detection systems are now being developed and implemented to answer the newly recognized threat of biohazards in the workplace. Additionally, chemical and explosive detection systems are being implemented at many facilities. Sophisticated air filtration systems are being developed to combat chemical threats from potential terrorists. Many of these newly developed technologies are already available and being implemented in those areas that the risks warrant such protection.

Safety and the safeguarding of personnel have always been a primary focal point for corporate risk managers. The hazards posed to facility personnel can range from the basic principles of clear egress paths to the more complicated protection from chemical and biological hazards found in the daily processes being utilized in many manufacturing and R&D applications. Prevention of hazardous situations is the first step in minimizing the risks and maximizing safety to personnel. Prevention methods may include: substitution of non-hazardous processes in place of a hazardous process when applicable, effective communication of the hazards to the facility personnel to enhance their recognition and response to these hazards, as well as effective communication to the local regulatory authorities. A secondary step to the prevention of hazards is detection, notification, and

control. Sophisticated monitoring and control systems have been developed and implemented in facilities requiring such systems. These include hazardous gas detection, fire detection, fire protection, emergency notification, and safety interlock and control systems. The third step in the prevention of hazards is contingency and recovery. How does a facility handle a hazardous chemical release? What contingencies are available to the facility should a hazardous situation occur? What recovery methods can be implemented in the event of a hazardous threat to safety? These questions can be answered in many different ways. However, each answer to these questions will include effective communication – to the employees, customers, suppliers, investors, regulators, and the entire community. Naturally, security and safety systems implemented for protection play an instrumental role in facility and personnel safety.

Conclusion

Risk management in today's evolving corporate environment has become more challenging than ever. The far-reaching effects of corporate globalization bring along uncertainty, both in the corporation's success and failure. The challenge for the risk manager is to identify these uncertainties, or risks, and determine the most effective method of managing the risks. Fortunately, the tools available to the risk manager have also evolved to meet these challenges. Numerous technical solutions have proven, and will continue to prove effective in managing and controlling risk. As technological advances continue to develop, the technical solutions available to the risk manager will become more sophisticated and effective. However, probably the most effective tools available to the risk manager are two basic principles that are beginning to make it back into most risk management programs – contingency and communication.

Contingency, in this context, encompasses more than just back-up plans or N+1 facility designs. Corporations are taking a serious look at equipping themselves with worst-case scenario financial contingencies. The removal of political, economic, and technological barriers to global corporate expansion has allowed corporations to extend themselves in ways never before imaginable. Conversely, this extension has brought many uncertainties to the corporation and its risk managers and insurers. These risks present serious challenges to those underwriting a corporation's risk management. Therefore, corporations are weighing the effectiveness of financial contingencies versus escalating costs of risk insurance.

Communication will prove to be the key to effective risk management in the coming decade. Over the past twenty years, corporations have become less reluctant to communicate their risks to the primary stakeholders for fear of deteriorating shareholder interests. The pattern is now changing. Corporations are realizing that poor communication to stakeholders has eroded confidence in their ability to effectively manage risk. Long-term effects of lost confidence of stakeholders are now being attributed to numerous corporate failures and are being found to far outweigh any short-term shareholder interests. Therefore, communication of risk management plans will be a key component to these plans.

References

Brown, R.V., *What Should Environmental Regulations Require: Specific Action, Acceptable Risk, or Cost Effectiveness?* Published paper, The School of Public Policy, George Mason University, 2000.

Kloman, H. Felix, Risk Management Reports, December 2000, Volume 27, Number 12.

USEPA, Chemical Accident Prevention: Site Security, EPA-K-550-F00-002, February 2000.

Kloman, H. Felix, Risk Management Reports, January 2002, Volume 29, Number 1.