

This article appears courtesy of Michael Hay, Director, Risk Assessment and Loss Prevention/Information Resources, State of Texas

Introduction

What is risk? One definition of risk is “a possibility of a variation of outcomes from a given set of circumstances.” Typically, risk carries a negative connotation and implies the potential for a loss of some kind. Since every activity within an organization involves taking risks in order to achieve an objective or make a profit, the only way to completely avoid risk is to do nothing! Normally, that is not an option. Therefore, it can safely be said that risk management should be present in every facet of business or governmental operations.

Within the past several years, the profession of risk management has emerged to better protect organizations from loss. Risk Management has many different definitions but all of the most current definitions identify a holistic approach to managing the risks of an organization known as “Enterprise Risk Management (ERM).” ERM is defined as “practice of protecting an organization from financial harm by identifying, analyzing, and controlling risk at the lowest possible cost.”¹ Interestingly enough, many of the new definitions of ERM also include aggressively managing risks to maximize the ability to profit from opportunities. Risk management is increasingly becoming involved in protecting organizations and maximizing potential for increasing efficiency and/or profit.

Logical Classifications of Risk

Since risk is inherent in every element of business operations, risk managers have identified a basic set of risk classifications under which a large variety of exposures, hazards, perils and losses may exist. These logical classifications are (1) Property (real, personal & intangible), (2) Human Resources (2nd party - i.e. employees), (3) Liability (3rd party – i.e. the public) and (4) Net income (any not otherwise categorized that could result in a loss of profitability).

In addition to logical classifications of risk, several key terms are used in order to administer a risk management program. Among the key terms used are the following:

Exposure – A situation, practice or condition which might lead to a loss, an activity or resource (assets, people).

Peril – A “cause” of loss; an event which may be the cause of a loss(e.g. fire, vandalism, etc.).

Hazard – A condition within an exposure that may lead to an accident, (i.e. “a peril about to happen” – e.g. the frayed electrical cord that started the fire).

Incident – An event that disrupts normal activities and may result in a loss or claim; “a near miss.”

Accident – An incident resulting in injury or damage to person or property which has or will become a loss or claim.

Occurrence – An accident with the limitation of time removed, often referred to as a progressive accident.

Loss versus Claim – Loss: A reduction in Value; Claim: A demand or obligation for payment as a result of a loss.

Frequency and Severity – Frequency: The number of times an incident occurs; Severity: The monetary impact of a loss.²

Maximum Probable/Possible Loss – Possible: the greatest amount an organization stands to lose resulting from a loss – Probable: the most likely amount an organization stands to lose from a loss.

Expected losses – Loss projections based on probability distributions and statistics; frequently developed using actuarial techniques.

Cost-Benefit Analysis (CBA) estimates and totals up the equivalent money value of the

¹ “The Practice of Risk Management”, The National Alliance Certification Manual

² “The Practice of Risk Management”, The National Alliance Certification Manual

benefits and costs to the community of projects to establish whether they are worthwhile. These projects may be dams and highways or can be training programs and health care systems.

The Risk Management Phases

Regardless of the class, risk management uses a systematized process for controlling risks. Whenever possible, every risk is subjected to following sequential process: (1) Identification, (2) Analysis, (3) Control, (4) Finance and (5) Administration³

Risk identification is the natural first step in the risk management process. Identification of risk is accomplished through any number of means. Checklists, work place walk-through, analysis of insurance policies, organizational chart analysis, financial statement analysis, loss data analysis and organizational policy and procedure review are some of the common means used to identify risks.

Once risks have been identified, they need to be analyzed to determine potential impact to the organization. Many types of analysis can be performed. Typically, the most relevant type of analysis will depend upon each type of risk being analyzed. While conducting risk analysis activities, the analysis should always remember that losses can be sustained from both direct and indirect sources internal and external to the organization. An example of a direct loss is the destruction of a building due to a fire. An indirect loss from the fire would be the loss of information on customers leading to a reduction in sales. It should also be remembered that both quantitative and qualitative losses can be experienced from the same event and that qualitative losses usually lead to quantitative losses.

While performing risk analysis, the analyst usually attempts to determine the projected frequency and severity of future losses as well as the maximum probable/possible loss that could result from them. These calculations assist the risk manager in determining the proper controls that should be implemented in

order to reduce the likelihood or impact of a loss, should it occur.

Risk control is the phase of the risk management process where assertive action is taken in order to reduce likelihood of a risk resulting in a loss or, at a minimum, reducing the impact of a loss. Essentially there are 5 techniques that are normally used to address or mitigate a risk, they are: (1) Retain the risk, (2) Control the risk, (3) Transfer the risk, (4) Avoid the risk and a (5) Combination of the other techniques.

When an organization decides to retain a loss, it has essentially accepted that a loss will occur and that the organization will finance (pay for) when it happens. Retention of risk is typically recommended for low frequency/low severity losses (see Chart 1).

Controlling a loss involves active intervention to prevent a loss from occurring or to lessen the impact of a loss should it occur. Examples of controlling a loss include developing policy to reduce exposures within an activity or providing personal protective equipment for employees engaged in handling toxic chemicals. This strategy is normally recommended for high frequency/low severity type losses.

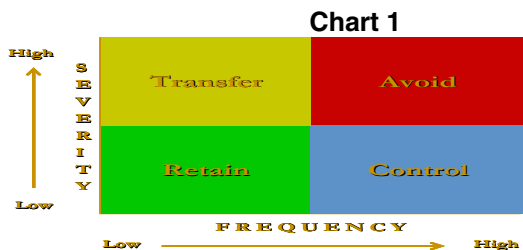
Losses that are low frequency/high severity in nature should normally be transferred. Transfer of a loss can take place physically or contractually. An example of a physical transfer of a loss could be demonstrated by getting another firm to perform a dangerous activity that has caused very few accidents to your employees, but they were extremely expensive. A contractual transfer occurs when you purchase insurance on a building. Losing a building to fire doesn't happen very often, but when it does it is extremely damaging (high severity) to operations.

Certain activities happen so frequently and are so severe in nature that the risk should be avoided. In the example above, instead of getting another firm to perform the dangerous activity, the activity would be eliminated altogether.

Finally, certain risks are best mitigated by implementing a combination of the other four strategies. You can get a general idea of

³ "The Practice of Risk Management", The National Alliance Training Materials.

which combinations could be used by looking at chart 1. The closer to any of the outside edges of the box a loss can be plotted, the stronger the indication for implementing that particular strategy. The more inward a risk plots within the grid, the more susceptible it is to using a combination of strategies.



The fourth stage of risk management is risk financing. This stage establishes the method(s) by which a risk will be paid for when it occurs. Risk financing is done either passively or actively. Passive risk financing acknowledges that all potential losses have not been identified and the organization will have to pay for them out of existing funds, should they occur. Active risk financing, on the other hand, identifies sources of potential loss and sets aside funds (reserves) or otherwise makes arrangements to pay for them.

The final stage of risk management is Risk Administration, which is the ongoing process of managing the risk management program. Risk administration also involves constant communications with management and employees regarding organizational exposures, mitigating strategies and ongoing loss experience.

Cost Benefit Analysis

It goes without saying that a company normally would not spend more money to mitigate a risk that it stood to lose from the loss itself. This principle applies across the board provided that maximum probable / possible loss calculations are accurately calculated and all direct and indirect exposures are considered. An example of this concept is the theft of a company computer containing confidential information. If maximum possible loss of the computer was improperly calculated on the value of the computer hardware alone, the result would be

low in value and might even indicate that the organization should retain the risk. If, on the other hand, the maximum possible loss of the computer was calculated based on the value of the hardware and a \$10 million judgment the company just paid resulting from the loss of the confidential data residing on a computer, an entirely different control strategy would emerge. Remember, it is important to identify and calculate as many direct and indirect costs of a loss as possible.

Managers need to constantly make risk management decisions and take action in order to protect their operations. Critical to the decision-making process is the need to compare the costs of mitigating a risk to the anticipated benefit. This process is known as Cost Benefit Analysis (CBA). CBA collects and compares inflows and outflows of resources and nets the difference between the two. Typically, if the net difference is positive, the project is acceptable. When many different projects yield a net positive result, the highest yielding projects are selected.

In order to perform CBA, several types of information must be made available. First, the amount at risk must be accurately calculated. Next, the time period over which the proposed control will apply must be known along with your organizations internal Weighted Average Cost of Capital (WACC - your CFO can give you this figure). Finally, the total cost of the mitigating strategy (including employee wages and benefits) must be obtained. For projects that are more than one year in duration, revenues and expenditures typically need to be discounted by the WACC. Discounting recognizes that funds earned or spent today have a different value than they will in the future due to inflation and other factors. You need to discount the cost or revenue in these calculations because money will be worth less in the future due to inflation. Expenditures need to be inflated as the organization could have invested the money and earned interest.. Once these numbers are developed, the simplified formula for calculating the cost benefit is:

$$(\text{Discounted revenue or reduced potential loss}) - \text{discounted cost to mitigate} = \text{net savings or net cost.}$$

Example:

Loss potential reduced by \$5,000

Risk Management

Cost to mitigate the risk is \$3,000 over 1 year
 Weighted Average Cost of Capital=10%

\$5,000 – (\$3,000 X 110%) = \$1,700 net savings

Usually any calculation yielding a net savings to the organization is acceptable therefore the above example would show a net benefit and would probably be accepted by management.

Risk Based Property Management

Historically, property management practices have been driven by the need to comply laws, regulations or accounting principles. The primary focus has been to demonstrate custody and stewardship of capitalized property items reporting to the financial statements, or that are required to be charged to a grant or contract. Consequently, many activities in property management have developed over time to meet these requirements, regardless of their cost effectiveness. Additionally, a very confined view of property risks has emerged over time, leaving many potential sources of loss unrecognized and unmitigated.

The fact that property is the first classification of risk emphasizes that it is amenable to the full risk management process. Further, since risk management is designed to protect an organization from many types of losses, use of a risk-based approach in managing personal property leads to a more holistic view and realistic analysis of true risks and potential losses to each property item.

Chart 2 below represents the lifecycle of personal property. Every phase of the lifecycle holds different risks for a particular piece of property or the property management program.

Chart 2 – The Property Lifecycle

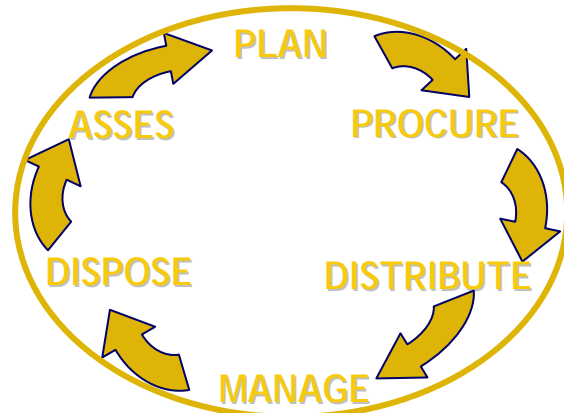


Chart 3 displays in greater detail some of the specific stages within the lifecycle that property is exposed to higher degrees of risk.

Chart 3
Phases of Life Cycle Exposed to Risk

- **Storage & Warehousing**
- **Maintenance**
- **Movement**
- **Subcontractor Control**
- **Physical Inventory**
- **Disposition**
- **Consumption**
- **Utilization**
- **Contract Closeout**

Let's take a look at a few of the specific perils associated with Chart 3 above.

Storage and Warehousing Perils

<u>Human Sources</u>		
Arson	Chemical Leaks	Contamination
Explosion	Embezzlement	Shrinkage
Error	Sabotage	Power failure
Temperature	Terrorism	Theft
Vandalism	Fire	Water
	Smoke	

<u>Natural Sources</u>		
Collapse	Corrosion	Evaporation
Rot	Rust	Mildew
Mold	Static Electricity	Vermin

<u>Economic Sources</u>	
Consumer Charge	Outdated Technology

Movement Perils

<u>Human Sources</u>		
Fraud	LDD	Error

<u>Economic Sources</u>		
Inaccurate Property Records	Underutilization	
Under Valuation		

Physical Inventory Perils

<u>Human Sources</u>		
Error	Embezzlement	Theft

<u>Economic Sources</u>		
Inaccurate Property Records	Under Valuation	
Inaccurate Financial Records		

The various types of risks and varying mitigating strategies for personal property are far too voluminous to discuss in this chapter. Additional training on risk-based property management can be received by attending NPMA seminars and training. For purposes of this chapter, we will only look at LDD risk management issues only for illustrating the identification, analysis, control and finance steps of the risk management process.

First, let's discuss identification. As you can see from the lifecycle perils, any number potential losses to property from any number of sources and perils. The question is "How do you identify them?" The answer lies in several places.

First, the property manager should look to the property system itself. If properly designed and maintained, the property system will contain a wealth of information on the acquisition, utilization and disposal of property. Included in this information should be details on any property losses that the organization has experienced.

Most modern property management systems support either querying or downloading of data into custom reports. In order to analyze your organizations LDD data, you will need to get a report or database containing your organizations historical property records. Information included in the database should, at a minimum, be property number, type or class of asset, date of purchase, historical value, estimated useful life, disposal date, disposal method, description, location, and responsible person or entity. In order to identify LDD property, it is necessary that your property system be designed to collect the above information and that there be some coding structure to identify such property.

Disposal Risks

<u>Human Sources</u>		
Chemical Leaks	Error	Contamination
Explosion	Fire	Theft
Violation of Disposal Guidelines		

<u>Economic Sources</u>		
Loss of Revenue	Loss of Good Will	

As you can see, various exposures exist in every phase of the property life cycle. Additionally, the same peril can exist in multiple places.

You will recall that the Risk Management Process involves 5 distinct steps: (1) Identification, (2) Analysis, (3) Control, (4) Finance and (5) Administration. Let's take a look at how these steps can apply to the property management program.

Once all LDD property has been identified within the property database, analysis can begin. During the analysis phase you need to determine the quantity and value of items within each class of property that is LDD. You also need to determine the period of time when and the location where the items were declared LDD.

For illustrative purposes, let's assume that all organization computers have the same

historical cost and, after analyzing LDD data over the past three years, you have been able to identify that 6% of the organizations desktop computers with a total historical cost of \$216,000 @ \$2,000 each, have been declared LDD each year for the past three years. Further, you have been able to determine that 2% of the computers were lost at the warehouse prior to being placed into service, 2% were lost in the medical building during utilization and 2% were located at the warehouse while being surplus. Finally, let's also assume that the LDD computers have been identified each year during the annual wall to wall inventory of personal property.

By the information provided above, we can calculate the frequency and one perspective of the severity of the computer losses for this sample organization. From the information provided above, we can calculate that the organization has a total of 1,800 desktop computers with a total historical cost of \$3,600,000 ($\$216,000/\$2,000=108$ LDD machines which represent 6% of total items and value----- 108 machines / $6\%=1,800$ total machines with $\$216,000 / 6\%=\$3,600,000$ total value). Remembering that frequency attempts to estimate the number of losses an organization will experience in the future, using simple linear regression techniques, we can estimate that, based upon the last three years losses, should the organization do nothing, it will probably once again lose 108 computers with a value of \$216,000.

Is this a significant problem? Are there too many LDD computers? Is \$216,000 the actual amount at risk for the organization? What are some risk mitigation options and are they cost effective? The answer to these questions is "it depends." It depends upon the managements appetite for risk, whether the computers were purchased as part of a grant, whether the organization is concerned about any negative publicity, etc.

The one thing that we do know for certain is that the current computer loss pattern is above the ASTM LDD standard for property. If the total for all personal property was also above the standard, this is ammunition for the property manager to use to convince management that something has to be done. Additional analysis can also be performed on

the data to help determine the financial and operation impact to the organization. For illustration purposes, let's assume the following loss locations have been consistent over the past three years:

Warehouse receiving – 36 LDD computers each year
Warehouse disposal – 36 LDD computers each year
<u>Med. Bldg utilization – 36 LDD computers each year</u>
Total 108 LDD per year

Now we know where the losses have occurred and in what phase of the life cycle they occurred in. The next question that we must now answer is "what is the maximum probable and maximum probable loss?"

The historical property management approach would generally assume that the maximum probable loss of amount at future risk would be \$216,000, which represents the historical cost of the forecasted 108 computers. The maximum probable loss would assume some form of disaster scenario such as the medical building burning to the ground and, incidentally where most of the computers are housed. Following this historical practice the maximum probable loss could be the number of computers in the medical building times the value per computer, i.e. $1,200$ machines X $\$2,000$ each = $\$2,400$ (maximum possible loss).

Since the frequency of the medical building burning down is very low and the severity would be very high, the standard mitigating strategy for this exposure (see Chart 1) would be to transfer the liability by purchasing insurance to replace the machines. On the other hand, we know that the frequency of the LDD computers at the medical building is $36/1,200=3\%$. This would indicate a medium frequency and low severity and might lead to the conclusion that additional controls such as increased inventories would need to be placed on the computers at the medical building (See Chart 1).

Using a risk-based approach for the computers at the medical building might yield an entirely different mitigating strategy. For example, what if two of the computers in the medical building have confidential information on them and the organization had just settled a lawsuit for breach of confidentiality resulting in a \$10 million judgment? In this scenario the

amounts at risk would change dramatically. For example the amount at risk in the medical building would skyrocket from \$72,000 (36 computers X \$2,000 each) to \$10,000,000. Safeguarding the organization from a potential \$10,000,000 loss is much more important than a \$72,000 one and calls for more stringent controls for those computers containing the confidential information. Remember, the computer itself is just the container for the confidential information but you as the property manager are responsible for protecting the container!

Sometimes innovative thinking needs to be applied to the solution. For example, where confidential information resides on a computer, perhaps locking the computer to the desk or wall might significantly reduce the risk of loss. This could be a simple and cost effective solution to eliminate the risk of the computer being stolen. Note however that this still would not protect the information from being copied to a disk and taken off site or being transmitted to another computer via the organizations email system.

Should the same control be placed on the LDD computers at the warehouse? Again, the answer depends upon the amount at risk posed by these computers. If confidential information does not reside on computers in the warehouse, then perhaps a different strategy could be implemented.

As we all know, there are any number of ways to reduce LDD exposure to property, some alternatives are more cost-effective and politically acceptable than others. Focusing on the warehouse, we will need to determine the most cost effective strategy to use in reducing the LDD property.

Suppose we were to build a cage to store all computers while in the warehouse? Assuming this would reduce the estimated loss to \$0, would this be a cost effective solution? In order to make this determination, it is necessary to perform a cost benefit analysis. As you will recall, the frequency forecast for computers declared LDD from the warehouse is 72. Up until now, we have dealt with a value based upon historical cost. In actuality, the most relevant value for determining the value of these machines is replacement cost for the new machines (in receiving) and the

average revenue from sales for the computers being disposed. For illustration purposes, let's assume that the replacement cost for computers is \$1,500 and the proceeds from sale of surplus computers is \$50 per machine. Given these numbers, 36 machines lost in receiving would cost the organization \$54,000 to replace and 36 machines lost during the disposal process would cost the organization \$1,800 in lost revenue. Therefore, if eliminate these losses, the organization would reduce losses by \$55,800.

Let's assume that the cost of building a caged area would cost \$10,000, would this be a cost effective strategy? Recalling that CBA calculates the inflows and outflows of resources, the CBA for this proposed strategy would be as follows:

Inflow (proposed saving) =	\$55,800
<u>Outflow (cost of strategy)=</u>	<u>\$10,000</u>
Net difference	= \$45,800.

Since the net difference between inflows and outflows results in a net savings, the proposed strategy would be considered cost effective. What if management was not willing to spend \$10,000 to build the cage, is there another cost effective strategy?

Let's assume that by increasing inventories from annual to quarterly we could reduce LDD by 50%. This would result in a loss reduction of \$27,900. How much would it cost the organization to implement the strategy? Chart 4 displays the current direct and indirect costs of the property management program and distributes these costs for each phase of the life cycle. Notice that the costs associated with the warehouse reveal 61¢ (Receiving - .05+Distribution - .08+Disposal - .48= .61). To calculate the costs it is necessary to apply the number of assets times the costs. In this case the number of assets as shown in Chart 4 is 600 X 61¢ X 3 additional inventories per year = \$1,098).

Applied to the CBA, the project effectiveness is as follows:

Inflows =	\$27,900
<u>Outflows =</u>	<u>\$1,098</u>
Net Difference =	\$26,802

As you can see, this proposal is cost effective. This proposal has the advantage of requiring no additional cash, just additional labor efforts from existing staff. The downside, however, is that the LDD property is not reduced as much as building a storage cage. You should also remember that the inflow calculations are based on projected figures. When performing CBA, it is always desirable to measure interim performance and savings and always report the final outcomes to management.

Costs of the Property Program

Every division and program within an organization has both direct and indirect costs associated with the cost of operations. Direct costs of the property management program consist of salaries and benefits for all personnel employed in the program plus the other expenses made for property management including contracted services, materials and supplies, capital outlay and any other expenditures made on behalf of the property management program. In addition to these direct costs, the property management program is supported by other divisions and the hierarchy of management. Even the CFO and CEO of the organization spend some time and energy on administering the property management program. All of the supportive costs are known as indirect costs and, although much less than the direct costs, they must be included in calculating the total costs of the property management program. Chart 4 found below breaks out the various costs of the program including both direct and indirect costs. Further, based on the number of property items in each phase of the life cycle, a cost per property item can be calculated for each phase of the life cycle as well as the total costs per property item for all phases.

Chart 4

Property Management Program Cost Data				
Direct Costs	Expenses	Allocation	Allocated Expense	
Payroll & Benefits	\$ 450,000	100%	\$ 450,000	
Contracted Services	63,000	100%	63,000	
Capital Outlay	125,000	100%	125,000	
Materials & Supplies	14,000	100%	14,000	
Miscellaneous Expense	5,000	100%	5,000	
Total Direct Costs	\$ 657,000		\$ 657,000	
Indirect Costs				
Management	\$ 1,165,000.00	2%	\$ 23,300	
Internal Audit	125,000	8%	10,000	
Risk Management	125,000	15%	18,750	
Total Indirect Costs	\$ 1,415,000.00		\$ 52,050	
TOTAL COSTS	2,072,000.00		\$ 709,050	
Annual Property Life Cycle Costs				
Total Cost Per Asset	\$ 4.54			
Life Cycle Frequency	Item Count	Allocation	Annual Cost	Annual Cost Per Asset
Receiving	1,659	1%	\$ 7,537.62	\$ 0.05
Distribution	2,900	2%	13,176.07	\$ 0.08
Utilization	135,000	87%	613,268.98	\$ 3.93
Disposal	16,500	11%	74,967.32	\$ 0.48
Total Property Count	156,059		\$ 709,050.00	\$ 4.54

Identifying Critical Property

Every organization has property that is critical to producing its products or delivering its services. Unfortunately, what has historically been considered critical property has been based mostly on historical cost or amenability to theft or misuse? As you can see from the previous examples, LDD is only one risk to personal property and focusing primarily on capital outlay items can cause an organization to miss some of its most critical exposures.

One prime example of this concept can be demonstrated in the Business Continuity Planning (BCP) process.

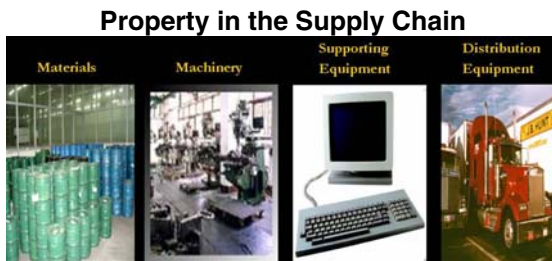
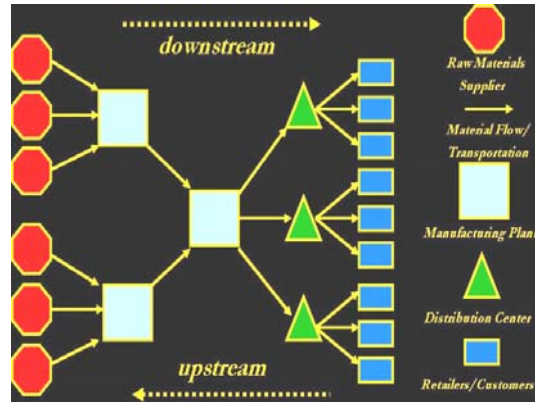
Business Continuity Planning is defined as *“the process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue without interruption or essential change.”*

Business continuity planning requires the organization to examine its critical processes and establish acceptable recovery time objectives in order to minimize the effect of disasters. As part of the identification of critical processes, it should be noted that most probably, the activities identified as most important require the use of property in order to achieve the desired outcome. The property manager therefore has a critical role in identifying those properties in the critical path of the organization and assuring their

availability or acceptable substitutes for use in recovering the business in times of crisis.

Property Risks in the Supply Chain

Another significant risk to the organization that involves property is the disruption of the organizational supply chain. A supply chain is defined as “a network of facilities that procure raw materials, transform them into intermediate goods and then final products, and deliver the products to customers through a distribution system”.



As you can see from the picture above, property is involved in every step of the supply chain. From the receipt and storage of raw materials all the way to distribution of product to wholesalers or retailers, personal property is used to facilitate movement from one phase to another.

Supply Chain Structure

Chart 5 illustrates the flow of assets through the supply chain. The chart illustrates the conversion of raw materials to finished product to delivery to retailers. This progression is known as “downflow.” The important concept to grasp from Chart 5 is that a failure in any phase of the cycle affects all processed down the line. Applying this principle to property management, any personal property system failure in a stage of the supply chain, will impact the integrity and efficiency of all subsequent stages. In other words, what superficially appears to be an isolated property issue can have an escalating effect on the organization through disruption of subsequent stages of the supply chain.

Understanding this important principle will assist the property manager in defining critical assets within the organization. It will also assist in determining appropriate mitigating strategies to reduce disruption to the business process supply chain.

Conclusion

The property manager has an integral role in the risk management process. Governmental and private sector forces are gradually moving property management from a compliance driven process to one that is risk based.

It is becoming increasingly important that the property manager have a fundamental understanding of the concepts used in risk management and apply them to cost-effective property management strategies to minimize loss and maximize opportunity for their organization.

*About Michael Hay, CRM, CGFM, CPPM
Mike is Director of Information Resources / Risk Assessment and Loss Prevention for the Texas State Office of Risk Management and currently the President of the National Property Management Association. He has over 25 years experience in business administration and property management for governmental entities and is a Certified Governmental Finance Manager and a Certified Professional Property Manager. Mike was an author of NPMA’s “The Standard Property Book – Asset Management for the New Millennium” and is frequently called on to speak throughout the nation on property and risk management topics.*