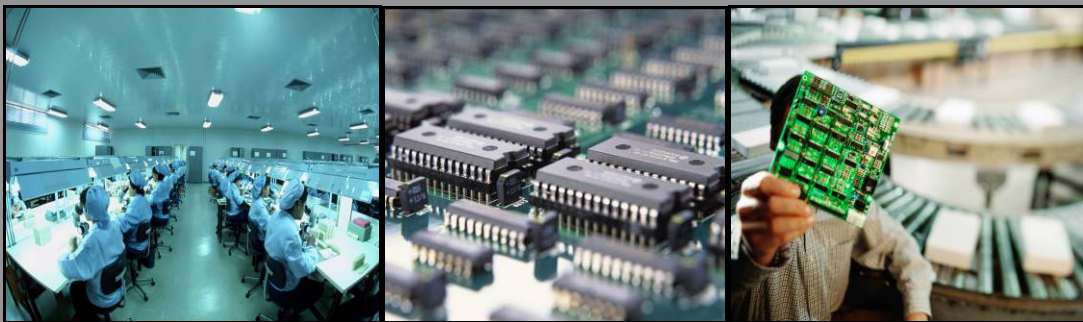




*Risk Control
Industry Guide Series*

Electronic Component and Hardware Manufacturing Industry



The electronics manufacturing industry is a complex supply chain reaching from the producers of inconceivably intricate circuit interconnections at the nano scale to the global web of interconnection of distributors, assemblers and original equipment manufacturers (OEMs). The increasing sensitivity of this supply network to unforeseen events rivals that of the global economy itself. This study uses analysis of electronics manufacturing industry insurance claims, industry trends and emerging loss exposures to derive suggested practices to manage risks that the industry is facing today and is likely to face in the future.

Electronics Manufacturing Industry Defined

For the purpose of this study, electronics manufacturing is broadly defined as:

- Electronic component and semiconductor manufacturing
- Electronic component and semiconductor distribution
- Computer, computer network equipment, and computer peripheral manufacturing

At the highest level, this industry encompasses operations that are part of the supply chain that produces physical devices to control the flow of electrons or combines these components into circuits to solve practical problems and serve useful purposes. Component manufacturers, distributors and circuit assemblers have unique and interlocking exposures to loss. The commonality of these exposures is partially due to the cascading dependencies of the supply chain and partially due to the cross functional nature of these organizations. In some cases, component designs are produced specifically for the end product in which they will be used, from packaging and form factor to firmware and environmental considerations. In other situations, assembly operations must carefully design circuit layout and processes for efficient use of commodity components, program micro controllers, and design and build enclosures to build a customized end product. Distributors serve as an important intermediary between component manufacturers and assemblers, not only offering increasingly precise supply chain management services but also as an important source of technical expertise. Electronic component distributors offer value-added services ranging from private labeling and kitting, to programming and engineering support. The convergence of the types of activities performed by manufacturers, distributors and assemblers increases the importance of taking a strategic view of managing risks to the supply chain as a whole.

The electronics manufacturing industry faces loss exposure from physical operations such as employee injuries, automobile accidents, liability claims and property losses, as well as unique exposures involving the services they offer and information that they handle. The following is a review of those exposures based on an analysis of claims incurred by electronics manufacturing companies insured by CNA between January 1, 2004 and December 31, 2007 and from industry data as indicated for some exposures where CNA data does not exist.

Workers' Compensation Claims

By Type of Incident Causing the Injury, Shown as a Percentage of Total Claims

Incident Type	Percent of Total Claims
Struck By or Against	33%
Manual Handling/Physical Stress	25%
Repetitive Motion	13%
Slips/Trips/Falls on the Same Level	10%
Caught	4%
Falls from Elevation	3%
Vehicle Accident	2%
All Others	10%

Shown as a Percentage of Total Claim Dollars

Incident Type	Percent of Total Claim Dollars
Manual Handling/Physical Stress	28%
Repetitive Motion	21%
Struck By or Against	18%
Slips/Trips/Falls on the Same Level	14%
Vehicle Accident	11%
Falls from Elevation	3%
Caught	2%
All Others	3%

This data indicates that the types of incidents most likely to cause worker injuries are manual handling and physical stress, repetitive motion and workers being struck by or striking against various objects. These three incident types also represent the highest severity of claims (cost in terms of claim dollars paid).

Manual Handling and Physical Stress

These claims were primarily caused by handling work-related materials, boxes and equipment. Leading type of work being performed when the injury occurred is related to manufacturing and assembly operations.

Repetitive Motion

As with manual handling claims, repetitive motion injuries are primarily attributable to workers in the manufacturing and assembly environment. Work involved handling various work-related materials, operating production machinery and working with tools.

Struck By or Against Object

This incident type is also associated with work in the manufacturing and assembly environment. Leading types of injuries in this category, in descending order, include lacerations, contusions, punctures, and foreign bodies (eye). Leading sources of lacerations were knives/cutters, machinery and sheet metal.

High Severity Workers' Compensation Claims – Over \$100,000 Incurred

Claims over \$100,000 represent approximately 20 percent of the total Workers' Compensation incurred losses. Leading causes of these high severity injuries were vehicle accidents, manual handling, and struck by or against incidents.

Property Claims

Incidents Causing the Loss, Shown as a Percentage of Total Claims

Incident Type	Percent of Total Claims
Burglary, Theft, Fidelity, V&MM	45%
Water Damage	18%
Fire	9%
Wind	9%
Hail Damage	2%
All Others	17%

Incidents Causing the Loss, Shown as a Percentage of Total Claim Dollars

Incident Type	Percent of Total Claim Dollars
Burglary, Theft, Fidelity, V&MM	53%
Hail Damage	19%
Fire	11%
Water Damage	7%
Wind	7%
All Others	3%

Property claims data show burglary, theft and other crime-related incidents such as fidelity and vandalism and malicious mischief claims as both the most frequent and highest severity type of loss.

Burglary and Theft

Approximately half of these claims involve the theft of stock, primarily computers, consumer electronics, computer peripherals and components. Business personal property items make up the balance, such as computers, office equipment and production equipment. Frequency and severity of theft losses appear to be a direct consequence of the industries primary products, ranging from memory chips and processors, to finished consumer electronics being highly attractive from a theft standpoint and small in size, allowing easier procurement and transport by thieves.

Over 80 percent of these incidents occurred at the organizations' premises. Common contributing factors included smash and grab style attacks, alarm systems being disabled, access from adjacent vacant spaces and possible insider involvement. The smash and grab incidents often involved using a vehicle to break through a roll up door or other barrier. Vandalism and malicious mischief losses are related to damage to buildings and equipment such as alarm systems.

Hail Damage

Though infrequent, hail damage can present high severity losses. Losses caused by hail include damage to roofing, HVAC units and water damage to building and contents.

Fire

Causes of fire losses include building electrical systems, heaters, and heating equipment used in production.

High Severity Property Claims – Over \$100,000 Incurred

Claims over \$100,000 represent approximately 45 percent of the total incurred property losses. These large losses include burglary and theft, fire losses and hail damage.

Auto Claims

Incidents Causing the Loss, Shown as a Percentage of Total Claims

Incident Type	Percent of Total Claims
Rear-ended Other Vehicle	18%
All Accidents Caused By Other Vehicle	13%
Struck Stationary Object or Vehicle	12%
Backing	10%
Lost Control of Vehicle – Left Road	4%
Changed Lanes	3%
Turned Left in Front of Oncoming Traffic	2%
Failed to Yield	2%
All Others	37%

Incidents Causing the Loss, Shown as a Percentage of Total Claim Dollars

Incident Type	Percent of Total Claim Dollars
Rear-ended Other Vehicle	31%
Lost Control of Vehicle – Left Road	15%
All accidents caused by Other Vehicle	13%
Backing	6%
Struck Stationary Object or Vehicle	5%
Changed Lanes	4%
Failed to Yield	4%
Turned left in front of oncoming traffic	2%

Analysis of auto claims indicates that one of the most preventable types of accidents, rear-ending other vehicles, as the leader in terms of frequency and severity

High Severity Auto Claims – Over \$100,000 Incurred

No auto claims over \$100,000 incurred.

Liability Claims

Incidents Causing the Loss, Shown as a Percentage of Total Claims

Incident Type	Percent of Total Claims
Damage to Property of Others	64%
Bodily Injury Caused by Operations or Products	36%

Incidents Causing the Loss, Shown as a Percentage of Total Claim Dollars

Incident Type	Percent of Total Claim Dollars
Damage to Property of Others	70%
Bodily Injury Caused by Operations or Products	30%

There are limited products- and operations-related liability claims found in the data used for this study. Damage to property of others caused by products or operations is the leading loss source in terms of both frequency and severity. Operations-related incidents are almost exclusively slip and fall of a visitor at the organization's business location.

Product Liability

Product liability claims account for 83 percent of the total incurred liability losses. Approximately three quarters of the total incurred product liability losses are related to physical damage to property caused by the products. Causes of damage include fires alleged to have been caused by products and defective circuit boards which caused customers to scrap their installed electronic components.

High Severity Liability Claims – Over \$100,000 Incurred

The only claim over \$100,000 involves the collapse of a communications tower for which the insured supplied an antenna.

Liability claims appear to be limited by the fact that electronics manufacturers have limited offsite operations, fewer visitors than many industries, and produce many products that are unlikely to cause direct bodily injury or property damage. It should be noted that product and service failures do occur, financial losses are sustained and claims are made against companies supplying these products or services. Loss experience in this area is examined in the next section which analyzes technology errors and omissions losses for this group.

Technology Errors and Omissions

Electronics manufacturing companies face an evolving array of risks rising out of their product and service offerings. While it is possible for electronic components and devices to cause direct bodily injury or physical damage such as electric shock or fire damage, these incidents are somewhat limited by the nature of the products and their uses. As mentioned in the preceding analysis of liability claims, only a limited number of these types of claims showed up in this study.

However, defects in components, devices or software embedded in these components and devices, can cause customers to lose revenue or incur significant financial expenses. For example:

- A component manufacturer is sued by a contract manufacturer or OEM for the cost incurred to rework, repair or recall product which was assembled using defective components supplied by the manufacturer. Damages can also include lost income and extra expenses incurred in implementing a work-around or in expediting repairs.
- Defense and settlement of consumer class action litigation alleging electronic products do not meet advertised specifications. This is common for complex end products such as computers, network equipment and cell phones. If defects in individual components used in these products are found to be at fault, the financial responsibility for responding to these complaints may work its way back through the supply chain.
- Custom designed electronics do not fulfill the expectations of the customer. This may be attributed to actual performance deficiencies, miscommunication about what the product functionality should be or changes over the course of product development about the product's function. Damages often include the cost associated with development of the product as well as lost income due to the fact that the customer still does not have a functioning product to utilize.
- Technical advice provided by a component distributor causes selection of components that are inappropriate for the specified use. Damages can be similar to those caused by supplying a defective component to the customer. Rework, process interruption and even recall from the end user may create significant customer expenses.

In general, errors and omissions incidents may arise for a variety of reasons associated with emerging technological innovation, expectation or legal interpretation of obligations. The most common reasons for such disputes include:

- Misunderstanding between buyer and seller
- Misrepresentation by vendors
- Acceptance of unrealistic specifications or changes in existing specifications without study or written agreement
- Acceptance of customers' risk through hold harmless agreements
- Failure to state performance obligations in contracts with the buyers
- Incompatible hardware or software
- Unusable recommendations by vendors
- Delays in project completion
- Failure to maintain disaster recovery plans or failure to back up, maintain or retain source code as required to protect buyer source data
- Security errors
- Violation of government laws or statutes, including intellectual property disputes that bar delivery of products or services as specified

Technology Errors & Omissions Loss Analysis

CNA data indicates a variety of complex causes of errors and omissions (E&O) claims with elements of the reasons listed above. Actual CNA claims parallel some of the examples given above including damages associated with rework of customer's product in which a defective component had been installed and failure of products specified by a distributor to meet customer requirements.

The data also indicates that the average E&O claim for this industry is \$202,670. The following chart compares E&O losses with those incurred by other types of exposure. While E&O claims are low in frequency, they can have a significant impact on a company's bottom line. Methods for controlling these risks should be included in an organization's overall risk management strategy.

Exposure	Average Incurred Loss
Technology Errors & Omissions	\$ 202,670
Property	\$ 33,255
Liability	\$ 17,570
Auto	\$ 5,095
Workers' Compensation	\$ 5,090

Information Risks

The emerging risks associated with handling large amounts of information have some unique characteristics and should be included in an organization's overall approach to risk management. The electronics manufacturing industry must precisely manage the massive amounts of data associated with component part numbers, specifications, product design information and globe spanning customer and vendor relationships. Inventory tracking and timely delivery to customers has direct measurable impacts on an organization's bottom line.

Due to current trends in privacy and information security, the industry's databases and information systems appear to be at significant risk. Network attack and information loss trends across all industries highlight some significant risks to the electronics manufacturing supply chain. This section of the guide will analyze available loss data and present potential loss sources related to first- and third-party information risks.

Information risks include threats to information technology systems, the intangible property handled by them and consequences of failure of these systems. These risks include first-party losses that would be sustained by the organization or third-party losses related to liability to others. Following are examples of these risks:

First-party Risks

- Loss of data
- Loss of business income
- Denial of service
- Virus/hacker/sabotage
- Theft of system resources
- Extortion

Third-party Risks

- Theft/disclosure of, damage to someone else's data
- Privacy injury liability
- Network security liability
- Content liability

These are events that may compromise the confidentiality, integrity or availability of an organization's electronic data or otherwise cause a loss of system resources. These same events may create liability to others in regard to data of others that is stored, handled or processed by an organization. As this is an emerging source of loss, there is limited insurance claim history which can be used for analysis. However, there is a growing public record of incidents related to security breaches of databases and private information they contain. The analysis below was created from a database of these public notices.

Privacy and Network Security Liability

According to data available from the Open Security Foundation, physical theft of devices such as laptops, hacking into systems and accidental release of sensitive information are indicated as the leading causes of breaches of sensitive or private, non-public information for manufacturers and distributors in general.

*Incidents by Cause of Security Breach — Manufacturers/Distributors***

Frequency (Percent of total number of breaches)		Percent of Total Records Exposed (Percent of total Records Exposed)	
28 Recorded Privacy Breaches		Approximately 1.1 Million Records Exposed	
Physical Theft (laptops)	62%	Physical Theft (laptop)	84%
Accidental (Web site)	14%	Hacking	10%
Hacking	10%	Employee Act	3%
Lost Media	7%	Accidental (website)	2 %
Employee Act	7%	Lost Media	<1%

January 1, 2004 to December 31, 2007 "DATALOSSdb" Open Security Foundation. October 16, 2008
<http://datalossdb.org/exports/dataloss.csv>

The information exposed in these breaches includes employee and customer sensitive or private non public information. Represented within this group are electronic component manufacturers and distributors of electronic components and devices. To date, privacy breaches have had much lower impact on manufacturers and distributors than industries such as financial institutions, healthcare and retail. Quite likely, this is due to the fact that, as a whole, the handling of the types of consumer information that has been the target of identity thieves is limited in these organizations. The primary concern for the electronics manufacturing industry should be that the same types of data leaks can contribute to the loss of sensitive information such as customer intellectual property. It should also be noted that there is a direct correlation between the hazards and controls related to these breaches and the exposures that can also cause first-party losses such as loss of data, loss of business income, and denial of service, theft of system resources, virus/malicious code incidents and extortion. To highlight these emerging threats, some claim scenarios are provided below.

- A circuit board assembler relies on its network to operate its production line. The network becomes infected by a computer virus which disrupts production and causes a delay in delivery of a customer's order. The customer sues the manufacturer for consequential damages, seeking recovery of late delivery penalties imposed by the customer's clients.
- A circuit board assembler stores its customer's design information on its network to support production of custom assemblies in accordance with customer specifications. A computer virus corrupts the customer's specifications. As a result, the contract manufacturer produces parts that deviate from customer specifications. This delays the customer's deliveries. The customer sues the manufacturer seeking recovery of late delivery penalties imposed by its downstream customer.
- An integrated circuit manufacturer uses its network to control production of custom chips. The production process includes preprogramming each chip with firmware designed for a specific customer. The firmware has passed all qualification testing and is under strict configuration control. As the final step in production, following final QA testing of IC devices, the manufacturer loads each device with customer-specific firmware from its configuration controlled source files. A virus infects the manufacturer's network, including the firmware source file. Each IC shipped is, in turn, infected by the virus. Customers install the virus-laden ICs in their own products. When the completed products are used by downstream customers, their networks are infected. The

manufacturer's customer must recall and replace all infected products. In addition, the customer is liable for damage to downstream customers' networks. The manufacturer's customers sue, seeking recovery of their product recall and replacement cost, their cost to defend lawsuits filed by downstream customers, and damages awarded to downstream customers for damage to their networks.

- An electronic component distributor uses its network to manage inventory and supply to customers. An employee who was denied a promotion hacks into the distributor's network and reduces inventory levels by changing resupply order triggers. As a result, the distributor's on-hand supply of component is not sufficient to meet customer production demands, causing delays in production. The manufacturer's customers sue the distributor seeking recovery of late delivery penalties imposed by their downstream customer and also sue for income lost due to their inability to fulfill customer orders.

Suggested Practices

The analysis of claim data presented here suggests basic practices that could be effective in reducing losses across exposure areas and specific practices that will reduce risk within a given exposure area. The electronics manufacturing industry has unique and emerging exposures but there is also insight to be gained from the common elements of exposures across other industries. The following are key insights derived from this combined data.

It is important to have a strategic approach to managing supply chain risks and consider the varied and unexpected forms of disruptive events and losses. By taking a holistic view of loss sources combined with emerging issues and business considerations for the industry, some key interconnections emerge:

- Leading cause of workers' compensation injuries are manual handling and repetitive motion related to work in the manufacturing environment. Product defects are the leading liability loss source. Supply chain disruptions caused by product defects are also the leading source of errors and omissions claims. There is a significant opportunity to not only affect these loss sources but also increase productivity and efficiency through focus on manufacturing processes and personnel.
- Theft losses are the leading property loss source as well as an emerging threat to intangible property (sensitive information). Physical security controls have a significant impact in both areas because, even for theft of sensitive information, the leading type of incident is physical theft of a device or media housing sensitive data. The key insight in both areas is that it is critical to segregate the high target items (be it memory chips or customer product design files) and provide the appropriate levels of protection.
- The complexity of the technology products produced and decision guiding technical advice provided by this industry is daunting and becomes more complex daily. Completing a business transaction in this environment requires careful attention to the potential unexpected consequences of the utilization of these technological innovations, customer expectation and legal interpretation of obligations. Contracts and agreements can help to define these expectations and provide protection from liability and limit damages.
- There are potential impacts to the supply chain from almost all of the loss sources discussed in this paper. Mitigating this impact and corresponding effect on your bottom line as well as that of your customers, requires formal incident response planning. A comprehensive approach which addresses disaster recovery, business continuity, product incident response and recall and even computer security incident response, is essential.

Implementation of a comprehensive risk management program is key to reducing Workers' Compensation, liability, auto and property losses.

- **Employee Safety** – Manual handling, physical stress and repetitive motion injuries are indicated as loss leaders in the analysis. An ergonomics program can protect workers from these types of injuries and increase productivity. Likewise, an effective safety program that raises employee safety awareness and helps to control and eliminate hazards will minimize the impact of other loss sources, such as slips, trips and falls.

CNA's ErgoPRO, a six-step ergonomic process that provides work method techniques, engineering guidelines and information required to integrate the human factor with the overall production process, and offers specific solutions to the frequent injuries related to the manual handling of materials. CNA's "Motion is Money" approach to ergonomics takes the subject to the next level by directly relating ergonomic concepts to measurable improvements in quality, productivity and profitability. CNA's other resources include guides and bulletins on worker safety recommendations and unique resources for loading dock safety.

- **Liability** – As noted in the analysis, product liability for direct bodily injury or physical damage to the property of others is somewhat limited by the nature of electronic products. However, this does not reduce the importance of addressing product liability hazards and controls for two primary reasons:
 - A thorough hazard analysis process may uncover bodily injury or physical damage potential which could go unrecognized. As the reliance on technology solutions to process and product control applications increases, so does its use in safety-critical applications, such as medical devices, industrial process control, transportation and security.
 - As previously noted, product and service failures do occur, financial losses are sustained and claims are made against companies supplying these products or services. The hazard analysis and controls associated with a product safety program address the core factors in preventing errors and omission losses: product development methodology and documentation, quality control and complaint handling.

CNA offers resources such as industry and exposure guides and bulletins to help limit liability through appropriate risk transfer techniques, premises hazards and product liability.

- **Auto** – Fleet safety is an essential part of any business' safety program. Even if the company does not operate a fleet of company-owned vehicles, few companies can operate without at least occasional business use of hired or non-owned vehicles by their employees. This analysis of electronics manufacturing industry claims indicates accidents in which the insured driver rear-ended another vehicle as the leading loss source in terms of frequency and severity of accidents. A fleet safety program that includes minimum driver qualifications raises driver safety awareness and implements driver accountability procedures that can have a tremendous impact on this type of preventable accident. The claim analysis also highlights the fact that automobile accidents often result in significant employee injuries.

CNA offers resources to aid in the implementation of a fleet safety program, including guides and bulletins on managing fleet safety and accident prevention and driver safety awareness.

- **Property** – A program for managing property risks is crucial in the prevention and mitigation of potentially catastrophic property losses. Property losses can have significant impact on all parts of the supply chain, through interruption of manufacturing and distribution processes and loss of work in progress, finished goods and production equipment. Property protection programs include

emergency response plans, self-inspection procedures and other special procedures related to hazard elimination and mitigation.

Two areas in which special emphasis and a broadening of scope of property protection programs are warranted to address the exposures of electronics manufacturing companies are:

- **Emergency Response Plans** – Plans should include disaster recovery, business continuity, product incident response and recall and computer security incident response. Together, these plans provide processes to recover from disruptions related to risks that may be natural, technological or human in nature. These plans serve to minimize interruptions to operations that not only may cause loss of business income but also liability or errors and omissions claims related to damage to property of others, loss of data of others and interruptions of supply of goods and services to customers.
- **Security** – Managing physical and information security should be a priority for the electronics manufacturing industry. In general, security for both tangible and information assets is about access control. Carefully crafted policies and procedures can address exposures to both types of assets. Sophisticated alarm systems and monitoring of network security have their place in the layers of protection that are needed, but for high target commodities, segregation and access control are critical. Countless losses have proven high-target assets stored and protected in the same way as other assets can leave them vulnerable, even with the most sophisticated overall protection. Instead, reliable controls applied to the most vulnerable assets, such as storing high-value components in a safe or storing employee data in a limited access encrypted database, are proven to provide solid protection with limited interruption to business processes.

CNA offers a variety of resources for the management of property risks. These tools include guides and bulletins on emergency response planning, property protection, and guidelines addressing both physical security and information risks. CNA has DRII certified Associate Business Continuity Professionals (ABCP) on staff, provides Infrared Thermography services, and assessments of privacy and network security risks.

CNA continually communicates about emerging issues and legal trends for the electronics manufacturing industry.

School of Risk Control Excellence

Courses applicable for the Electronic Component and Hardware Manufacturing Industry:

- Electronic Component and Hardware Manufacturing Boot Camp** – Addresses industry loss drivers from a safety and industrial practice viewpoint
- Building Your Business Continuity Plan (BCP)** – Covers elements necessary in a BCP strategic plan to help restore and keep critical business functions going within the first 72 hours of a disaster
- Case Management — A Partner with Workers' Compensation** – Addresses techniques to maximize the delivery of healthcare and return-to-work outcomes
- Concepts of Business Continuity Planning (BCP) Overview** – Addresses how to create an effective BCP that can help ensure your business survives the impact of a disaster
- Elements of an Effective Product Liability Prevention Program** – Identifies 13 elements of an effective product liability prevention program
- Emergency Planning** – Provides guidelines for developing and implementing emergency plans at various facilities
- Emergency Planning: Equipment Breakdown, Business Interruption, and Commercial and Industrial Manufacturing** – Provides specific guidelines for developing and implementing emergency plans at locations where there is equipment breakdown exposure
- Emerging Threats to the Electronic Components Supply Chain** – Discusses risk control techniques for preventing or mitigating losses and strategies for transferring residual risk
- Fire Protection, Inspection, Testing and Maintenance** – Discusses NFPA 25 requirements for inspection, testing and maintenance of fire protection systems
- Flammable Liquids** – Discusses classification of liquids, storage requirements including Maximum Allowable Quantity (MAQ) in various occupancies and fire prevention techniques
- Infrared (IR) Thermography** – Explains the science behind IR, potential benefits that can help reduce costs by reducing losses
- Manage Chemical Health Risks to Protect Your Employees and the Company's Liability** – Explains the effect that chemicals in a product might have on the health of employees
- Nanotechnology** – Provides an overview of nanotechnology, including current facts related to potential health and safety risks associated with nanomaterials
- Privacy and Computer Network Security Risks** – Provides participants tools and resources to effectively recognize and manage computer network risks
- Return-to-Work (RTW) Process** – Explores the elements of the RTW process and workers' compensation requirements
- Warehousing – Controlling Your Property Exposures** – Analyzes sprinkler systems to help make informed business decisions to maximize the ability of the fire prevention system

To learn more about how CNA Risk Control can work with you to help you mitigate risks, please speak with your local independent agent, call us toll-free at 866-262-0540, or view our Risk Control tools online at www.cna.com/riskcontrol.

The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situations. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. Any references to non-CNA Web sites are provided solely for convenience and CNA disclaims any responsibility with respect thereto. CNA is a service mark registered with the United States Patent and Trademark Office. Copyright © 2008 CNA. All rights reserved.