Telecommunications Industry
This study reflects on information derived from insurance claims.

These claims form a database that can be analyzed to determine the many and varied causes of loss. CNA Risk Control presents this study of specific CNA claims and industry trends. We begin with a review of exposures inherent to the Telecommunications Industry and conclude with suggested practices to manage these risks.
Telecommunications Industry Defined

Telecommunication networks have evolved to become the backbone through which we conduct our daily lives and transact our business. The operation of this complex infrastructure involves risks of loss ranging from damage to the infrastructure’s physical components, such as towers and switching equipment, the corresponding interruption of services provided to worker injuries, and liability claims associated with maintaining these networks. This study uses analysis of telecommunication 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.

For the purpose of this study, the telecommunications industry is defined as wired and wireless service carriers, and resellers. “Convergence” has blurred the line between wired telephone service carriers and cable technologies. In cases where high capacity cable networks are used to carry phone and data services in addition to television services, cable are also included in this category. Likewise, wired and wireless network carriers are not differentiated according to the traffic they carry, voice, data, television programming, music or movies.

One of the primary factors which affects loss exposures facing companies in this category is that the network infrastructure must be extended to customers over a geographically widespread area, be that regional, national or international. Equipment such as towers, antennae, switches and lines including copper, fiber optic and coaxial cable must be constructed, operated and maintained in remote, publicly accessible and sometimes harsh environments. Network endpoints are in customer locations which require installation of equipment in homes and businesses. The fact that a significant portion of the industry’s customer base is individual consumers increases exposures related to retail sales of products such as mobile phones, the protection of large databases of private, nonpublic consumer information, and the sensitivity of consumers to installation and repair procedures performed in their homes.

Telecommunications: An Analysis of Loss Exposures in the Telecommunications Industry

As a whole, the telecommunications 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 telecommunication 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

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Percent of Total Claims (3,563)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Handling/Physical Stress/(+lifting)</td>
<td>20%</td>
</tr>
<tr>
<td>Slips/Trips/Falls on the Same Level</td>
<td>19%</td>
</tr>
<tr>
<td>Repetitive Motion</td>
<td>14%</td>
</tr>
<tr>
<td>Struck By or Against</td>
<td>14%</td>
</tr>
<tr>
<td>Caught</td>
<td>3%</td>
</tr>
<tr>
<td>All Other</td>
<td>25%</td>
</tr>
</tbody>
</table>
Shown as a Percentage of Total Claim Dollars

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Percent of Total Claim Dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Handling/Physical Stress/(+lifting)</td>
<td>23%</td>
</tr>
<tr>
<td>Slips/Trips/Falls on the Same Level</td>
<td>22%</td>
</tr>
<tr>
<td>Falls from Elevation</td>
<td>17%</td>
</tr>
<tr>
<td>Repetitive Motion</td>
<td>14%</td>
</tr>
<tr>
<td>Vehicle Accident</td>
<td>8%</td>
</tr>
<tr>
<td>Struck By or Against</td>
<td>8%</td>
</tr>
<tr>
<td>Caught</td>
<td>1%</td>
</tr>
<tr>
<td>All Other</td>
<td>7%</td>
</tr>
</tbody>
</table>

The data indicates that the types of incidents most likely to cause worker injuries are manual handling and physical stress, slips, trips and falls on the same level, and repetitive motion. Manual handling and physical stress, slips, trips and falls on the same level, and falls from elevation represent the highest severity claims. Leading type of work being performed when the injury occurred is field service, maintenance and installation of network infrastructure.

**Manual Handling and Physical Stress**

These incidents were primarily caused by the handling of boxes, tools and equipment such as ladders, and work-related materials such as wire.

**Slips, Trips and Falls on the Same Level**

Slips, trips and falls on the same level occurred on all types of walking and working surfaces at company facilities and offsite locations.

**Falls from Elevation**

Falls from elevation were primarily related to falls from stairs, ladders, utility poles and work around open manholes and trenches.

**High Severity Workers’ Compensation Claims – Over $100,000 Incurred**

Claims over $100,000 represent approximately 25 percent of the total Workers’ Compensation incurred losses. Leading causes of these high severity injuries were falls, manual handling, and vehicle accidents.

**Property Claims**

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

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Percent of Total Claims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burglary and Theft</td>
<td>56%</td>
</tr>
<tr>
<td>Water Damage</td>
<td>15%</td>
</tr>
<tr>
<td>Wind Damage</td>
<td>11%</td>
</tr>
<tr>
<td>Fire</td>
<td>4%</td>
</tr>
<tr>
<td>Snow/Ice Damage</td>
<td>1%</td>
</tr>
<tr>
<td>All Other</td>
<td>13%</td>
</tr>
</tbody>
</table>
Shown as a Percentage of Total Claim Dollars

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Percent of Total Claim Dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wind Damage</td>
<td>64%</td>
</tr>
<tr>
<td>Burglary and Theft</td>
<td>21%</td>
</tr>
<tr>
<td>Water Damage</td>
<td>8%</td>
</tr>
<tr>
<td>Fire</td>
<td>2%</td>
</tr>
<tr>
<td>Snow/Ice Damage</td>
<td>2%</td>
</tr>
<tr>
<td>All Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

Property claims data shows wind damage as the highest percent of total claims and also a leader in terms of frequency of occurrence. Burglary and theft is the most frequent type of loss and also a leader in terms of total percentage of property losses.

Wind Damage

Wind damage was related to hurricanes occurring in the southern United States.

Burglary and Theft

Over 60 percent of the theft losses are related to theft of mobile phones at retail sales locations associated with wireless carriers and service providers. Business personal property items make up the balance, such as computers and office equipment. Common contributing factors included smash and grab style attacks, alarm systems being disabled and access from adjacent vacant spaces.

Water Damage

Primary causes of these water damage incidents were plumbing leaks and heavy rains.

High Severity Property Claims – Over $100,000 Incurred

Claims over $100,000 represent approximately 80 percent of the total incurred property losses. These large losses include wind damage, water damage, burglary and theft; and snow and ice causing a communications tower collapse.

Auto Claims

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

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Percent of Total Claims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rear-ended Other Vehicle</td>
<td>34%</td>
</tr>
<tr>
<td>Backing</td>
<td>32%</td>
</tr>
<tr>
<td>Struck Stationary Object or Vehicle</td>
<td>10%</td>
</tr>
<tr>
<td>Failed to Yield</td>
<td>5%</td>
</tr>
<tr>
<td>All accidents caused by Other Vehicle</td>
<td>1%</td>
</tr>
<tr>
<td>All Other</td>
<td>18%</td>
</tr>
</tbody>
</table>
Analysis of auto claims reveals 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

Claims over $100,000 represent approximately 20 percent of the total incurred auto losses.

Liability Claims

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

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Percent of Total Claims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage to Property of Others</td>
<td>63%</td>
</tr>
<tr>
<td>Bodily Injury Caused by Operations or Products</td>
<td>33%</td>
</tr>
<tr>
<td>Personal Injury*</td>
<td>4%</td>
</tr>
</tbody>
</table>

*Offenses such as slander, libel and invasion of privacy

These claims primarily involve operations conducted off-site at the customer’s or another location. The work being performed when the incident occurred includes field service, maintenance and installation of network infrastructure. Claims that did occur on company premises are largely due to customer slips, trips and falls at retail locations associated with mobile phone sales.

Bodily Injury Caused by Operations or Products

Although claims against organizations alleging bodily injury caused by their operations or products represent only one third of the incidents, the severity of these claims represents over half of the total incurred costs. The majority of these incidents involves job site operations and includes incidents such as being struck by materials or equipment, and slips, trips and falls.
Damage to Property of Others

Property damage incidents are also primarily job site related. There is a high frequency of minor property damage to homes and contents of subscribers during installation of products or extending services to homes. Higher severity incidents tend to involve utility damage, water damage to customer homes as a result of damaging interior water lines, fires and other damages cause by network equipment.

Product Liability

Incidents in which products caused bodily injury or physical damage are limited in terms of frequency and severity. Types of incidents include bodily injury and physical damage related to mobile phones, chargers and other network equipment installed in homes.

Personal Injury

The data includes claims of invasion of privacy and defamation.

High Severity Liability Claims – Over $100,000 Incurred

Claims over $100,000 represent approximately 35 percent of the total incurred liability losses. All of these high severity incidents are job site related.

Technology Errors & Omissions

Telecommunication companies face an evolving array of risks rising out of their product and service offerings. Software code can contain security vulnerabilities that allow hackers to penetrate customers' networks. Allegations of software copyright infringement are increasingly common. Defects in network design, software, and hardware can cause customers to lose revenue or incur significant financial expenses.

Errors and Omissions (E&O) 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 limited E&O claims activity for telecommunications companies. The claims do indicate a variety of complex causes with elements of the reasons listed above. Telecommunications companies’ E&O risks increase according to the complexity of their service offerings, which increasingly includes information technology services ranging from systems integration to custom network design. Modern
telecommunications systems also serve as distribution means for traditional broadcast media, music and movies. Production of custom content, licensing and digital rights management issues can expose telecommunications providers not only to E&O claims but also to information risks which are discussed further in the following section.

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. Over the past few years, privacy injury liability has become a significant concern for many industries, and the telecommunication industry is no exception. In CNA analysis of publicly available information on privacy breaches across all industries, telecommunication companies are breached about 40 percent as frequently as retail operations and actually rank higher in terms of severity of breaches than healthcare organizations.¹ This result comes as no surprise, considering that at least 50 percent of the industry’s customers for telephone service are consumers² causing the industry to handle and store types of information that has been the target of identity thieves. This section of the guide will analyze available loss data and present potential loss sources related to first-party 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. Some examples of these risks are given below.

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 the telecommunications industry.
Incidents by Cause of Security Breach — Telecommunications Companies

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent of Total Records Exposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Records Exposed</td>
<td>Approximately 4.8 Million Total</td>
</tr>
<tr>
<td>Hacking</td>
<td>86%</td>
</tr>
<tr>
<td>Lost Media</td>
<td>13%</td>
</tr>
<tr>
<td>Lost / Stolen devices (laptops)</td>
<td>1%</td>
</tr>
<tr>
<td>Employee Act</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Accidental (website)</td>
<td></td>
</tr>
</tbody>
</table>

18 Recorded Privacy Breaches

- Lost / Stolen devices (laptops): 33%
- Hacking: 22%
- Accidental: 22%
- Lost/Stolen Media: 17%
- Employee Act: 6%


The information exposed in these breaches includes employee and customer sensitive or private nonpublic information. Represented within this group are wired and wireless telecommunications companies. As discussed above, privacy liability is a leading information risk exposure but 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, denial of service, theft of system resources, virus/malicious code incidents and extortion. Network breaches may also result in liability to others for improper use of licensed content or intellectual property of others may be infringed upon by content created by a telecommunications carrier. The impacts of these types of incidents in terms interruption of normal operations and liability for damages to others warrants careful attention to these risks in a telecommunications company’s overall risk management strategy.

Suggested Practices

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

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 falls 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, 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. This process could offer specific solutions to the frequent injuries related to the manual handling of materials and equipment during network installation and maintenance activities.

  CNA’s FallPRO, a seven-step process to identify, evaluate and control exposures when working at heights, can be used to address the variety of fall exposures encountered by the telecommunications industry.
CNA’s other resources include guides and bulletins on Workers’ Compensation and office ergonomics. These outline specific issues that affect the telecommunications industry’s workforce and how to alleviate environmental factors.

- **Liability** – An effective safety program also helps to control and eliminate hazards that may cause bodily injury or physical damage to others, creating liability for an organization. As the analysis shows, these incidents can occur on company premises but for the telecommunication industry are primarily associated with installation and maintenance activities at off-site locations. The scope of the safety program should address premises exposures, as well as the exposures created by off-site operations, such as telecommunication line work in public areas and work in and around customer residences.

CNA offers resources such as industry and exposure guides and bulletins to help limit liability through appropriate risk transfer techniques, control of premises hazards and job site safety.

- **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 telecommunication 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. As with workers’ compensation and liability claims, the majority of auto accidents are related to network infrastructure installation and maintenance.

A fleet safety program that includes minimum driver qualifications raises driver safety awareness and implements driver accountability procedures 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 a telecommunication company’s ability to deliver services without interruption. 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 telecommunication companies are:

  - **Emergency Response Plans** – Plans should include disaster recovery, business continuity, 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 E&O claims related to damage to property of others, loss of data of others and interruptions of services to customers.

  - **Security** – Managing physical and information security should be a priority for the telecommunications industry. In general, security for tangible and information assets is about access control. Carefully crafted policies and procedures can address the exposures to both types of assets.

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 also 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 telecommunication industry.
School of Risk Control Excellence

Courses applicable for the Telecommunications Industry:

☐ 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
☐ Contractor Utility Disruption – Offers precautionary practices to follow prior to the start of any underground work
☐ FallPRO – Outlines steps for implementing a comprehensive fall protection process for the leading cause of fatalities in the construction industry
☐ Fire Protection, Inspection, Testing and Maintenance – Discusses NFPA 25 requirements for inspection, testing and maintenance of fire protection systems
☐ Infrared (IR) Thermography – Explains the science behind IR, potential benefits that can help reduce costs by reducing losses
☐ 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
☐ Telecommunications Boot Camp – Addresses industry loss drivers from a safety and industrial practice viewpoint
Footnotes

   http://datalossdb.org/exports/dataloss.csv

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.