Texas Council Risk Management Fund

# Risk Advisor

Spring 2015

## What is Cyber Liability Insurance?

News stories appearing almost every day tell us about serious breaches of computer systems or the release of thousands of customer names and information. Major national companies like Target, Kohl's, Anthem Healthcare and Sony have been hacked in the past year or two with tremendous damage and cost to repair. When this epidemic of attacks started the usual perpetrator was an individual or small group that seemed to be motivated by the same thrill vandals get when they deface property or spray graffiti. Now, because the information stolen from companies is so lucrative when sold, large groups, sometimes sponsored by national governments engage in breaching companies and engaging in cyber terrorism verging on outright war. The recent attack on Sony Entertainment in Hollywood has been traced back to North Korea. Their attack was in response to Sony's approaching release of a movie that lampooned that country's leader, Kim Jong Un. The attack destroyed thousands of company computers, released all of the corporate e-mails, confidential medical information about employees, unreleased movies and reduced the company to communicating in a pre-computer mode. Sony reverted to land lines, the mail and handwritten memos delivered by messengers within the company until reliable computer service could be restored. According to the Insurance Journal "the cost to Sony from new software, hardware, employee cost to clean up the mess, investigators, lost productivity and reputational damage is at least $100,000,000 and growing."

The attack on Sony involved planting malware in Sony's system to mine data for about a month before all of their computers simultaneously displayed a "screen of death" graphic and froze. At this point the computer hard drives were wiped and the hardware was disabled. This scenario could happen to any company or community center creating the same kinds of expenses to recover, repair and resume operations. Most community centers have software protecting against viruses, malware and hacking. Most centers use encryption, firewalls, complex passwords and limitations to data access. However, as computer experts tell us, no system is immune from a cyber breach by determined hackers. As we know from the breaches of large retail and healthcare companies, the financial incentive is individual identities to sell and credit card numbers to exploit. According to one computer person interviewed for this report identities taken from a company's data system can bring as much as $150 each. The hacker does not care where the identity information came from; it is all sellable. Another target of hackers is the personal health information that healthcare organizations possess. According to Katherine Keefe, Group Leader of Breach Response at Beazley (a provider of cyber liability insurance) in "Fierce CIO, The Executive IT Management Briefing," health data such as name, age, physician and diagnosis can be used to fabricate a new medical identity to use to defraud Medicare or Medicaid. Another, even more lucrative use of this data is to sell to unscrupulous physicians who use it to write prescriptions for narcotics which they then sell.

Community centers generally do as much as their limited resources permit to prevent and deter cyber attacks. But what can be done after an attack occurs? The exposure of personal health information (PHI) and other confidential personal information can create a huge potential liability for a center under HIPAA and other statutes. The rapidity and effectiveness of a response to any breach is crucial in mitigating and reducing risk.

see **Cyber Liability Insurance** on page 4

IN THIS ISSUE

# Loss Control Briefs

## Upcoming Liability Workshops Scheduled

The Fund has three liability workshops scheduled during the remainder of 2015. Please mark your calendar for the following dates.

- July 10, 2015—"Risk Management Foundations for Executive Leadership," Austin, Texas at the Westin Domain. This workshop is designed for executive leaders who are new to their positions and will provide a historical perspective on the development of the community center system, risk management best practices, information on how to deal effectively with boards and other on target topics for new leaders. Presenters will include Brian Crews and Mike Winburn.
- September 24, 2015 – "Property and Casualty Claims Workshop," The Omni Southpark, Austin
- October 23, 2015—"Integrated Care – Recent Developments with added Legislative Update," The Menger Hotel, San Antonio

Information concerning workshops will be mailed to centers several weeks in advance of the events. The Fund's web site also provides workshop information and online registration. (**www.tcrmf.org**--" Workshops and Training" page).

## Upcoming Safety Workshops Scheduled

Here is the current schedule for regional safety seminars during Spring/Summer 2015.

- June 4, 2015, Corpus Christi
- June 24 and 25, 2015, Houston
- July 9, 2015, Fort Worth

The workshops are designed for center safety officers and others with safety and risk management responsibilities. Both new and experienced staff will benefit from this program. This one-day seminar addresses current safety issues and provides guidance for managing community center safety programs. Presenters will discuss specific problems being encountered by Fund members and offer practical solutions to help reduce accidents and resulting losses. The course will be conducted by safety professionals of the Texas Council Risk Management Fund. Topics include:

- Site Safety Officer (Roles and Responsibilities)
- Selling Safety to Management and Staff
- Hazard Identification and Correction
- Accident Analysis

For further information about Liability and Safety Workshops, contact Renee Harris at Renee.Harris@yorkrsg.com or 800-580-6467.

see **Loss Control Briefs** on page 5

Texas Council Risk Management Fund




## Risk Advisor

**Volume 27, Number 2**

Published quarterly by the Texas Council Risk Management Fund.

Questions, comments, tips, advice, ideas, opinions, criticism, and news are welcomed and encouraged. Every effort has been made to ensure the accuracy of the information published in *Risk Advisor.* Opinions on financial, fiscal, and legal matters are those of the editors and others. Professional counsel should be consulted before taking any action or decision based on this material.

Fund Administrator: York Risk Services Group, Inc.

800-580-6467

# Hurricane Season Already?

On May 6, 2015 the National Hurricane Center designated an area of disturbed weather near the Bahamas and Florida as Invest 90 meaning an area to watch for possible tropical cyclone development. The system moved north and impacted the coasts of South and North Carolina. This is one of the earliest declarations of an invest in the Atlantic but does this indicate an active hurricane season?

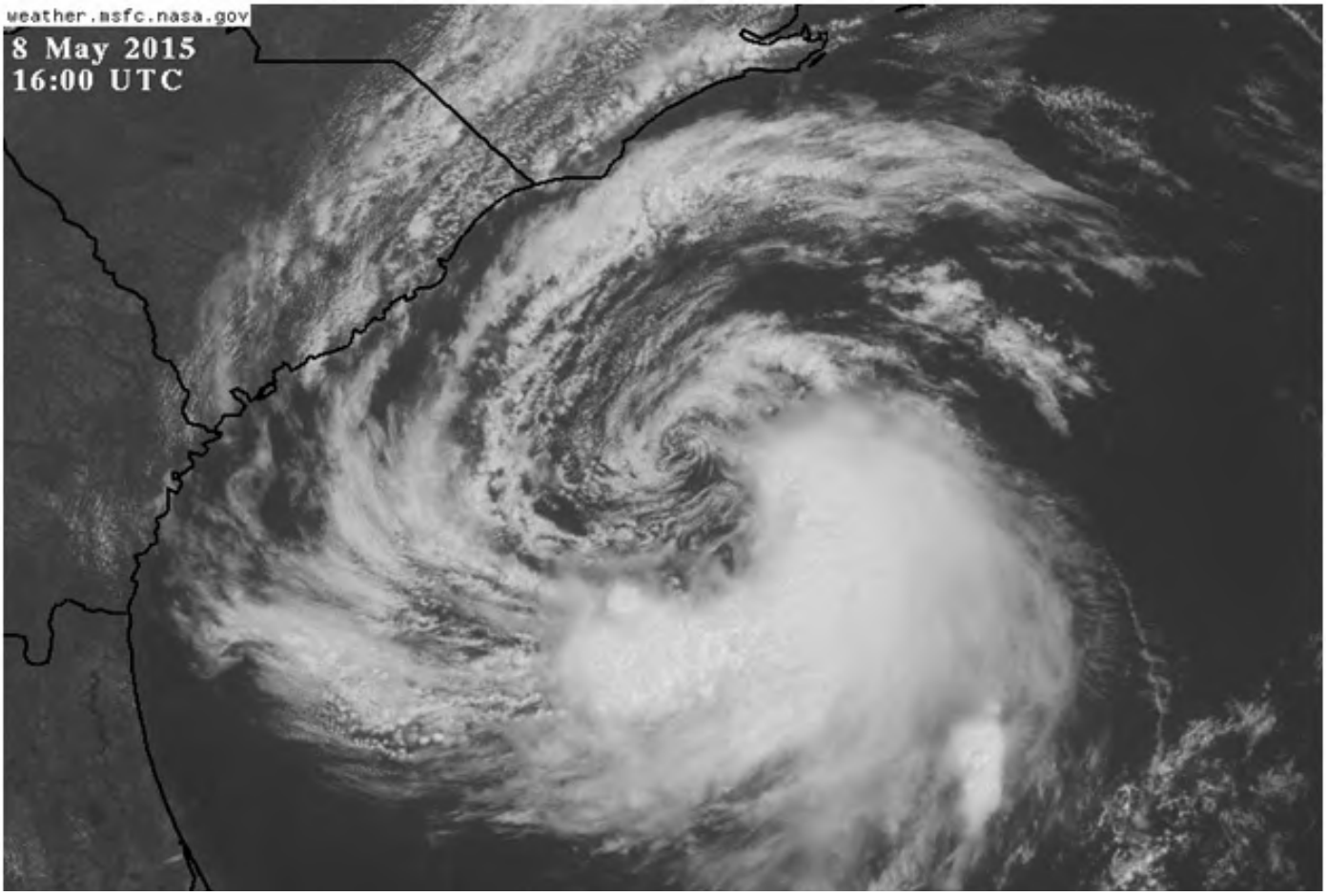
According to the Tropical Meteorology Project at Colorado State University the 2015 season will be below normal for formation of tropical storms in the Atlantic basin. Their "Extended Range Forecast of Atlantic Seasonal Hurricane Activity and Landfall Strike Probability for 2015" predicts seven named storms including three hurricanes with one of those reaching "major" status or between the Category 3 and 5 storm strength. They also predict a 15% probability of a storm strike along the Gulf coast from the panhandle of Florida to Brownsville, Texas. The usual average is 30%.

There appear to be a couple of major reasons for the low estimate of tropical cyclone activity. One of them is the relatively cool sea surface temperatures in the eastern Atlantic where storms first begin to develop after they come off the continent of Africa. In early May those temperatures were running one to three degrees Celsius below normal. Tropical storm development usually requires temperatures above 80 degrees (26 degrees Celsius) and sea surface temperatures in the area of primary storm formation off the coast of Africa is only in the 70's.

Another main reason for a lower estimate of the number of storms is the presence of an El Nino in the Pacific Ocean. El Ninos cause a west to east wind flow over the Gulf of Mexico and the Caribbean that creates wind shear above tropical cyclones. The wind shear tears off the tops of thunderstorms in the cyclone and weakens potential development. The wind shear can tear storms apart or reduce their intensity significantly.

There is, however one other factor present in May of 2015 that could lead to the formation of storms in the Gulf of Mexico. Sea surface temperatures in the Gulf are higher than normal so storms could form in the Gulf and move quickly over the coast anywhere from the Rio Grande delta to the southern tip of Florida. These storms can be a real problem because the preparation lead time available to coastal residents is much shorter than a storm that has been tracked all the way across the Atlantic Ocean.

Centers should monitor any tropical development, update storm response plans and be ready to protect people and property in the event a tropical storm heads your way. As Dr. Gray at Colorado State says, "Despite the forecast for below average activity, coastal residents are reminded that it only takes one hurricane making landfall to make it an active season for them. They should prepare the same for every season, regardless of how much activity is predicted."




*Sub-tropical storm Ana from NOAA and National Hurricane Center on May 8, 2015*

**Loss Control Briefs ,** continued from page 2

## Laptop Computer Security

According to industry sources, hundreds of thousands of laptop computers were reported stolen or missing last year. Although the loss of an expensive asset like a computer is a serious concern, the loss of the data contained in the laptop is often more important and valuable than the computer itself. Following are some suggested elements of a laptop security policy:

- Provide written security guidelines for physical protection of laptops in the office and when traveling.
- Provide annual training and periodic reminders to maintain safety and security awareness.
- Communicate in writing the policies and procedures regarding employee accountability for the safety and security of laptops assigned to them.
- Consider making loss of a laptop by gross negligence a performance issue that could result in disciplinary action up to and including termination.
- Encourage users to back up their files frequently.
- Maintain a current list of all laptop users, assigned equipment, serial numbers, and software. Audit the list annually.
- Conduct both regularly scheduled and random inventory checks.
- Investigate all incidents of theft or accident and publicize the results internally.
- Make employees aware that all thefts will be reported to the police.
- Make sure that all data transmission is encrypted.
- Consider software that will "wipe" the data stored or lock the computer if an unauthorized user attempts to gain access or the laptop goes missing.
- Consider use of tablets that cannot be used to download client files and only operate as "dumb" terminals when accessing the client files on the center's servers.

## Extension Cord Safety

Centers often use extension cords to overcome deficiencies in number and placement of electrical outlets in their facilities. Fund Loss control consultants often encounter extension cords across the floor, dangling from ceilings and creating potential trip or fire hazards. The U.S. Consumer Product Safety Commission estimates that each year about 4,000 injuries associated with extension cords are treated in hospital emergency rooms. About one-half of the injuries involve tripping over cords. Following are some tips for safe use of extension cords:

- Use extension cords only when necessary and only on a temporary basis. Permanent wiring should be installed for permanent workstations and equipment.
- Inspect cords for physical damage before use.
- Check the wattage rating on the appliance or tool that the extension cord will be used with. Do not use a cord with a lower rating than the equipment to be energized.
- Do not allow extension cords to run through standing water or get wet.
- Make sure that all equipment and extension cords bear the mark of an independent testing laboratory such as Underwriters' Laboratories.
- Keep cords off the floor where they might cause a tripping hazard or be rolled over or crushed.
- Keep cords away from places they might be caught in moving equipment.
- Keep cords out from under or over doors and away from moving objects that can wear off their insulation.
- Don't run cords through holes in ceilings, walls, or floors.
- Don't run cords under rugs or carpets or in high traffic areas.
- Pull on the plug, not the cord when removing a cord from an outlet.
- Don't move, bend, or modify any of the metal parts of the extension cord plug. Do not cut off the grounding plug to fit in a two slot receptacle. This defeats an important safety feature that can prevent serious injury or fire.

Consult with your Loss Control Consultant if you have any questions about the safe use of extension cords in your facilities.

## Hail

Spring in Texas can be beautiful and horrific on the same day as sudden changes in weather occur. Recently an outbreak of severe weather caused tornados, hail and flooding in large areas of north and northeastern Texas. Tornados are the most dangerous and destructive of the natural hazards facing most centers, but hail is a close second and much more widespread. Some of the largest claims paid by the Fund over the years have been hail claims that have devastated vehicles, roofs, windows and the walls of buildings. Property claims adjusters for the Fund have the following recommendations for members in the event of hail:

- Even fairly small hail can cause damage. Report any hail event to the Fund so we can have an expert examine your buildings and vehicles for damage.
- Contact the Fund first before you make any arrangements with roofers or auto repair shops. After a hail storm roofers flood the telephone lines and even go door to door promising new roofs, free upgrades, no deductibles and free estimates. The first step is to report the claim and allow the Fund to guide you through the process to make sure reputable and reliable roofers and auto repair shops do the repairs.

see **Loss Control Briefs** on page 5

**Loss Control Briefs,** continued from page 4

- Protect property from further damage. If the roof leaks or windshields are broken, protect contents from further water damage.
- If you can safely do so, get pictures of the hail and note the date and time of the event.
- Hail damage that is not visible initially can appear over time and cause a roof to leak months or years after the hail storm. If there is hail damage and a claim is paid, have the roof fixed. If a claim was paid but the repair was not done, future damage may not be covered.

## Earthquake

Texas is not known as a very active earthquake zone, unlike large parts of the West Coast or the northern Rockies. However, there has been an alarming swarm of small earthquakes in the north Texas area associated with the Barnett Shale oil and gas drilling boom. Several earthquakes in the range of 2.5 to 4.0 on the Richter scale have been experienced in the counties surrounding Fort Worth since 2008. On May 7, 2015 an earthquake registered 4.0 on the Richter scale and caused some minor damage in Mountain Creek about 35 miles southwest of Dallas. The current hypothesis about the cause of the quakes proposed in a study by SMU is that the re-injection of produced salt water and its extraction from producing wells is causing an increase in underground fluid pressure leading to slippage along old, inactive fault lines. Well fracking occurs over a very small area surrounding the well bore, but salt water disposal wells pump huge volumes of water thousands of feet underground into large formations. This can affect large areas as the salt water pushes out from the injection point. Most oil and gas wells in the Barnett Shale field produce up to 100 barrels of salt water per day along with hydrocarbons.

In response to the earthquake activity in North Texas Fund members have asked about coverage for earthquake damage to their buildings. Generally, the grant of coverage is "all risk of physical loss of or damage to property arising from an occurrence…except as hereinafter excluded." In the "Perils Excluded" section earthquake is listed as one of the perils excluded from coverage. There is an important exception for fire or explosion that ensues after an earthquake. Damage caused by the fire or explosion only would be covered. The Fund is examining the possibility of providing some coverage for earthquake damage. This involved process includes consultation with the reinsurance company and determining limits of liability and what contributions to charge.

*Sources: Fort Worth Star Telegram, Salt Water Disposal Wells, November 18, 2007, Natural Gas Intelligence Newsletter, April 21, 2015, Associated Press reports, May 7, 2015*

**Cyber Liability Insurance,** continued from froint cover

Other than maintaining sufficient staff or contractors to respond to a breach an effective measure is cyber liability insurance that can help a center contain the damage, respond to a breach and address the liability issues raised by release of data.

Cyber liability insurance first began to appear about 15 years ago as computer systems began to gather more and more personal information and the criminal mind began to see the potential for monetary gain. Now the market for cyber insurance is growing at a double digit rate each year as companies look for ways to handle the liability created by criminal data mining. The cyber liability insurance policy usually consists of two major sections. The first section is a breach response feature that helps a center respond to a breach as soon as it is detected. It is considered a "first party" coverage because it provides services to the community center to respond to the breach event. The second major section is liability insurance for the potential damages done to the people or entities whose confidential information is released. The liability section also responds to the fines and expenses related to HIPAA or other law violations created by a breach. These are "third party" coverages for the center's clients who are affected by the unauthorized release of their confidential information.

The liability or third party coverages include:

- **Information security and privacy liability** for damages and claim expenses due to the theft, loss or unauthorized disclosure of personally identifiable information. Information that the center possesses that belongs to another organization and for which the center is liable through a contract or business associate agreement is also covered.
- **Regulatory defense and penalties** will pay on behalf of the center claims expenses and penalties assessed because of regulatory proceedings for violations of privacy laws caused by an insured incident.
- **Website media content liability** pays damages and claims expenses as a result of the display of false or defamatory information on a center's website. Types of actions covered include libel, slander, infliction of emotional distress, harm to reputation, violation of rights to privacy, plagiarism, copyright infringement and other related offenses.
- **PCI fines, expenses and costs** provides a limited amount of coverage for expenses and costs related to a release of electronic cardholder data. This coverage is primarily designed for credit card information, but as centers increase billings to private parties there could be more exposure to this hazard.

Limits of liability may go up to $5,000,000 and there is retention (deductible) usually around $5,000 per incident. Claims have to be reported in writing and must occur during the policy period for there to be coverage. There are also exclusions for occurrences that would be covered by other kinds of insurance, the result of criminal or dishonest actions of the insured or claims because of violations of

see **Cyber Liability Insurance** on back cover

Texas Council
Risk Management Fund
Risk
ADVISOR

P. O. Box 26655
Austin, Texas 78755-0655

## Cyber Liability Insurance, continued from page 5

ERISA, war, pollution and other causes. Claims may also be denied if data being transmitted is not encrypted.

Perhaps the most valuable feature of Cyber Liability Insurance is the provision of "Privacy Breach Response Services." This is one of the insuring agreements in the policy but it is also an on call and immediate reaction to notice that a center is experiencing a breach of its information systems. The breach response service includes:

- Computer expert services that will pay the cost of a computer security expert to "determine the existence and cause of an actual or suspected electronic data breach" that would require the center to comply with a Breach Notice Law. The expert would also determine the extent of unauthorized access to data.
- Legal services provided by attorneys skilled in breach response and notification matters.
- Notification services will provide notification to individuals who are required to be notified of a breach required by a Breach Notice Law and to individuals whose information has been stolen that poses a significant risk of "financial, reputational or other harm to the individual."
- Call center services will be made available for a period of 90 days to respond to inquiries from people affected by the breach by providing them with information about the incident and information required to be provided by HIPAA or other applicable laws.
- Breach Resolution and Mitigation services will provide credit and identity monitoring for individuals affected by the breach.
- Public relations and crisis management includes cost for a crisis management consultant, up to $100,000 for media purchase or mailing materials to inform the public about the breach and other costs of notification and repair and restoration of affected records.

The breach response is coordinated by specialists who have extensive experience in responding to data breaches. Their approach is to respond to the breach first, then sort out what liability issues arise because of the breach later. The breach response unit retains expert contractors who can respond quickly to a call for help. After the breach is resolved and a course of action determined all of the other liability coverages could come into play if harm to individuals or organizations caused by the breach triggers the coverages.