Texas Council
Risk Management Fund

Risk Advisor

Winter 2016

Cyber Pirates

In early February 2016 the Hollywood Presbyterian Medical Center in Los Angeles was hit by a ransomware attack. Ransomware (also known as cryptolocker) is an insidious piece of software that gets inserted into the victim's operating system as an e-mail attachment or hitchhiker in a thumb drive. The attacking software methodically encrypts all of the internal files it can access, shuts down the system and posts a demand for payment in order to provide the key to decrypt everything. When the attack hit, the hospital was no longer able to access patient electronic medical records, operate computer based diagnostic equipment like MRI's or operate their pharmacy. The initial demand for ransom was $3.6 million in "bitcoins," an untraceable form of payment.

In response to the attack initial efforts by the hospital's IT staff were unsuccessful in restoring their system. So, hospital staff resorted to telephones, fax machines, written notes and paper patient records. One doctor noted that the biggest obstacle to going back to a paper record was the notoriously bad handwriting by physicians. No patients were injured during the attack, but several pacemaker and MRI patients were transferred to other hospitals. Overall, there was no access to CT scans, lab work, drug dispensing robots or electronic patient or medication records. By February 18 the hospital paid a ransom of $17,000 as the quickest and cheapest way to restore their system.

IN THIS ISSUE

see **Recent Cyber Attacks** on back cover

Coming Events

The Fund Presents the Revised 2016 Line-up of Liability Workshops for Texas Community Centers

- April 29, 2016: The Emergency Response, **the Westin Galleria, Houston, Texas,** Recent terrorist acts in the United States and France have put a spotlight on safety and security of center staff, clients and facilities. This workshop will present key information about how to respond to emergencies, basic principles of facility security, recognizing indicators of workplace violence, drills and training for effective emergency response.
- July 08, 2016: Purchasing Fundamentals and Risk Management, **the Westin Domain, Austin, Texas,** Statutory purchasing and performance contract purchasing requirements will be reviewed. Methods of procurement for real estate, goods and services, ethics and public information act requests arising out of purchasing activities will also be discussed. Cautionary tales and purchasing war stories will be told.
- October 21, 2016: Confidentiality Issues, **The Menger Hotel, San Antonio,** Confidentiality issues continue to be frequent and troubling issues for community centers. The important aspects of preventing confidentiality problems will be presented.

All hotels listed above will honor state rates for rooms as long as reservations are made before their deadlines. Specific rates and deadline dates will be provided when the flyers for each workshop are issued. Workshops will begin at 8:00 a.m. and conclude by 3:30 p.m. A continental breakfast and full lunch will be served with snacks in the afternoon.

Continuing Education Credits

The Fund has continuing education sponsor agreements with the Texas State Board of Examiners of Social Workers, the Texas State Board of Examiners of Professional Counselors, the Texas State Board of Examiners of Marriage and Family Therapists and the Texas State Board of Public Accountancy. Continuing Education credits may also be applied for from the State Bar, HRCI and the Texas Department of Insurance for specific workshops.

Registration is Easy

Register online at tcrmf.org. There is a nominal fee for members and a slightly higher fee for non-members. Registration includes workshop materiaks, breakfast, lunch and snacks in the afternoon. Workshops begin at 8:00 am and conclude by 3:00 pm.

Texas Council Risk Management Fund

Risk Advisor

Volume 28, Number 1

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

Loss Control Briefs

Gun Sign Update

Many districts/centers have had questions about the new gun laws that went into effect in Texas in 2016. The article in the Fall 2015 Risk Advisor had basic information about the signage requirements of the law. Since then some members have been approached by members of the public about their signage. Simple removal of the signs is all that is required by the law unless there is a refusal and the matter is referred to the Texas Attorney General. That's when failure to remove a sign could get very expensive. To date, there are no known instances of a member referral to the Attorney General. Center staff should know how to call 911 if someone enters a center facility and "displays a firearm or other deadly weapon in a public place in a manner calculated to alarm" as stated in the Texas Penal Code, section 42.01 (a) (7) & (8). With new phone systems and a greater reliance on cell phones it may not be as simple to dial 911 as it used to be.

Top 10 Questions about the Fund's New Workers' Compensation Claims Submission Process

York Risk Services Group, the administrator of the Texas Council Risk Management Fund recently converted all Fund claims to a new claims system effective October 1, 2015. The new system is referred to as York Claims Expert A (YCEa). To facilitate the conversion of all historical data into the new system, the old system went down effective September 18, 2015 and was down for approximately five working days. The claims team planned and prepared for the system being down to minimize any disruptions.

In December 2015 and January 2016, the Fund conducted approximately 8 webinars with over 40 members participating introducing the new claims submission process. The introduction included 2 new systems:

- iCOW which is used to submit First Report of Injuries, DWC-1 only and
- YCEa, which is used to submit DWC-3 and DWC-6 forms.

Information regarding all these changes is documented on the TCRMF.org website, under the *Claims Forms and Notices* section and *Workers' Compensation Form* tab. This area provides direct links to iCOW and YCEa, written instructions to each system (with screen shots) and instructions on how to manually complete the DWC forms.

During this introduction and transition, we have received several questions and wanted to address those questions at this time.

1. What is the difference between iCOW and YCEa?

- iCOW is used to submit a DWC-1, First Report of Injury **only.** YCEa is the claims system used to administer and manage claims for the Fund. Members have access to review claims and submit DWC-3 and DWC-6 through YCEa.

2. How do I get access to iCOW and YCEa?

- Past users who submit claims on behalf of the member should have received a userid and password already. However, if you did not receive a userid and password, you can go to www.tcrmf.org, under the *Claims Forms and Notices section and Workers' Compensation Form* tab and click on **"New User Access: Click here to request access to YCEa (and iCOW)"**. This is a PDF form that needs to be completed and then emailed to Janina.Flores@yorkrsg.com.

See **Top 10 Questions** on page 5

The Zika Virus

The World Health Organization has declared a Health Emergency in response to the rapid spread of the Zika Virus. The virus was first discovered in equatorial Africa in 1947 while researchers were exploring the jungle canopy for yellow fever in Rhesus monkeys. The first human case detected was in Uganda in 1952. Large recent outbreaks have occurred in French Polynesia in 2013 and Brazil in 2015(and ongoing). The disease has spread throughout South and Central America and is being introduced into the United States by infected travelers from those areas.

Media reports as of February 2, 2016 indicate that the mosquito borne infection caused by the Zika virus may be sexually transmitted. A person in Texas has been infected with the Zika virus after having sex with an ill person who had returned from Venezuela according to the Dallas County Health Department. The virus appears to be moving into the United States from Latin and South America. Cases have been reported as far north as New York City in persons who have recently traveled to South America. The virus is carried by the most common mosquito species that inhabits the southern United States, the Aedes aegypti. The Zika virus has gained much notoriety because it appears to cause a very damaging birth defect know as microcephaly, abnormally small skull development in newborns. The frequency of microcephaly went from fewer than 400 cases reported in Brazil in 2014 to over 4,000 reported in the first four months of 2015. The disease has also been associated with the potentially paralyzing Guillian-Barre Syndrome. The World health Organization also notes that Guillian-Barre Syndrome was prevalent during the outbreak in French Polynesia in 2013. These associations are strongly circumstantial but scientifically unproven at this time.

The usual symptoms of infection include relatively mild flu-like symptoms such as mild fever and headache, joint and muscle pain, a rash and red eyes (conjunctivitis). The symptoms usually last from two to seven days. The disease has been reported in over 34 countries worldwide with 26 in the Americas. The World Health Organization has noted that it is "spreading explosively" with over 1.5 million cases reported in Brazil. The Texas Department of State Health Services recommends that people should protect themselves from mosquito bites by:

- Wearing long-sleeved shirts and long pants
- Using EPA-registered insect repellents
- Using permethrin-treated clothing
- Staying and sleeping in screened-in or air-conditioned rooms
- Avoiding or limiting outdoor activities during peak mosquito times
- Protecting young children and the elderly who cannot take measures to protect themselves

The mosquito is active during the day and a couple of hours before and after sunset. The Centers for Disease Control has recommended that pregnant women should avoid travel to affected areas as well as taking the precautions mentioned above. At present there is no vaccine.

World Health Organization Bulletin, Texas Department of State Health Services

Top 10 Questions, continued from page 3

3. Are the username and password the same for iCOW and YCEa?

- Yes, the same username and password are used for both systems.

4. When I am in iCOW entering a claim it asks me to select the type of claim to open, can I enter a General Liability or Automobile Liability claim?

- No, not at this time. iCow is used to submit workers' compensation claims **only**.

5. When entering the claim in iCOW I get a screen that says, "The Employer has more than one type of policy. Which type of claim are you making?" What do I select?

- Select "Workers' Compensation – State Workers' Compensation Act". Do **not** select, "Workers' Compensation –Employer's Liability".

6. I don't have a userid/password and I need to send a DWC form to the adjuster immediately?

- Go to www. TCRMF.org website, under the *Claims Forms and Notices section and Workers' Compensation Form* tab. Once there, you will see, "Manual Form: Click here to submit a manual DWC Form-1 email to: OSCTexas@yorkrsg.com." You will see similar links for the DWC-3 and DWC-6. When you click on the link, a PDF form will pop up where you will type the information. Once complete, save the document and email to OSCTexas@yorkrsg.com. OSC Texas is our mail room where we enter the claim into the system and assign it to the appropriate adjuster.

7. I am locked out of the system and need to reset my password?

- If you are locked out of the system and need to reset your password, please contact Janina Flores at Janina.Flores@yorkrsg.com and/or Kathy Hulse at Kathy. Hulse@yorkrsg.com. We will work with our IT department to get you reset.

8. I have tried to get into YCEa and on the first screen it asks for my Login, Password and Company. What do I enter for Company?

- You will enter "JIC" as the Company name.

9. How do I find a particular claimant/claim?

- You will enter YCEa and the first thing you will need to do is locate the claim. You will look on the left side of the screen and select the "Search" button. This screen will then give you options to search. If you have the claim number, you will enter that. If you have the "old" claim number that would start off with "W020," you would enter that under the "Legacy Claim Number." The last option is a search by First and Last name of the claimant.

10. Once I have the claim I need, how do I submit a DWC-3, Wage Statement?

- Once you have the claim up on the screen, on the top you will select the folder named "Functions." On the "Claims Functions" page, you will look for the heading "Miscellaneous." Under that heading, select "Forms and Letters." Once selected, enter "DWC" in the search engine and select DWC-3.

Texas Council
Risk Management Fund
Risk
ADVISOR

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

Cyber Pirates, continued from front cover

Investigators believe that sloppy passwords or reckless human behavior may have opened the hospital to attack. Since the first of the year three other hospitals have been attacked in a similar manner. To help prevent ransomware or any other kind of cyber-attack, centers should exercise a strict password protocol that includes complex passwords that are changed on a regular basis. They should also train and establish policy prohibiting the use of thumb drives from outside sources or the opening of e-mail attachments unless from a known source. In addition, centers should have an "Incident Response Plan" that will allow them to continue vital functions in the event of a ransomware attack or other disruptive event. Experts also recommend that an affected center

- Quickly acknowledge the breach
- Don't insult the public by claiming that no client information is at risk
- Don't call it a random attack. The attackers pick their targets.
- Don't pay the ransom if there is another way to recover.
- Notify law enforcement.

The Hollywood Presbyterian Medical Center only acknowledged the breach after several days of struggle. Their public announcement claimed that no patient records or lives were at risk and that they were a "`random" target. They eventually paid the ransom, then called law enforcement.

Effective system back-up is even more important in a ransomware attack. Both data and software systems should be backed up regularly and frequently. You may lose some recent data, but it is better to reconstruct a day's worth than lose it all or pay an exorbitant fee to criminals.

Finally, don't think it can't happen to you. In 2014 a member center experienced a ransomware attack and the awful consequences of trying to restore services to their clients. All operations of the center were disrupted and the lack of effective back up left the only solution a payment of the extortion demand.

Sources: Yahoo News, February 16, 2016; Chronicle Council, February 23, 2016; EMS World, February 18, 2016