THE POOL CUE

MICHIGAN COUNTY ROAD COMMISSION SELF-INSURANCE POOL
Volume XIX Issue 2 May 2013

MCRCSIP MISSION STATEMENT

"The Mission of the Michigan County Road Commission Self-Insurance Pool is to administer a self-insurance program and to assist members with risk management efforts."

COUNTY ROAD COMMISSION INSURANCE CONFERENCE

We are pleased to inform you that the County Road Association Self-Insurance Fund and the Michigan County Road Commission Self-Insurance Pool will be holding their annual membership meetings at the Soaring Eagle Resort in Mt. Pleasant on July 24th and 25th.

The schedule is as follows:

Wednesday, July 24th

9:30 - 11:30 CRASIF Loss Prevention Program
11:30 - 12:30 Lunch
12:30 - 2:30 CRASIF Annual Business Meeting
2:30 - 3:00 Break
3:00 - 5:00 MCRCSIP Workshop

Thursday, July 25th

7:30 - 8:15 Breakfast
8:30 - 11:30 MCRCSIP Annual Business Meeting

Check in is from 7:00 a.m. to 3:00 p.m. on Wednesday and from 7:00 a.m. until 8:30 a.m. on Thursday in the corridor outside of the Swan Creek Saginaw Room.

You can register for one or both meetings using our online registration form at **www.mcrcsip.org** or **www.crasif.org**.

The cost of registration is $25 per person and includes both the MCRCSIP and CRASIF programs, lunch and dinner on Wednesday, and breakfast on Thursday morning. Please be sure to register by July 2nd.

For those of you desiring lodging at the Resort, a block of rooms has been reserved. You can make your room reservation online by going to **www.soaringeaglecasino.com**. Our group number is 9940II. The Soaring Eagle also needs your reservation by July 2nd.

We look forward to seeing all of you in July!

IN THE CUE

Page

COMPENSATORY TIME FOR PUBLIC EMPLOYEES

Wendy S. Hardt, Attorney
Michael R. Kluck & Associates

Recently, the Working Families Flexibility Act was introduced in Congress. The bill would allow non-exempt private sector employees to opt for paid time off in lieu of payment for overtime hours. Employees would earn compensatory time off ("comp time") at a rate of at least one and one-half hours per hour of overtime worked, up to 160 hours per year, and would be able to cash out any unused, accrued comp time at the end of each year.

Under the Fair Labor Standards Act ("FLSA"), public employees may already receive compensatory time off at a rate of not less than one and one-half hours for each overtime hour worked instead of cash payment for overtime, under certain prescribed conditions. Specifically, in order to utilize such comp time, there must be a collective bargaining agreement, memorandum of understanding or other written agreement put in place before the performance of the work. Compensatory time is capped at 240 hours for most public employees under the FLSA. After reaching that cap, the employee must be paid overtime compensation for any additional overtime hours of work.

An employee who has accrued compensatory time off and who has requested use of such compensatory time must be permitted by the employer to use such time within a reasonable period after making the request if the use of compensatory time does not unduly disrupt the operations of the employer. Whether a request to use compensatory time has been granted within a "reasonable period" will be determined by considering the customary work practices within the employer based on the facts and circumstances in each case. Such practices include, but are not limited to (a) the normal schedule of work, (b) anticipated peak workloads based on past experience, (c) emergency requirements for staff and services, and (d) the availability of qualified substitute staff. Mere inconvenience to the employer is an insufficient basis for denial of a request for compensatory time off. The employer must reasonably and in good faith anticipate that it would impose an unreasonable burden on the employer's ability to provide services of acceptable quality and quantity for the public during the time requested without the use of the employee's services.

If compensation is paid to an employee for accrued compensatory time off, such compensation must be paid at the regular rate earned by the employee at the time the employee receives such payment. An employee who has accrued compensatory time off authorized to be provided shall, upon termination of employment, be paid for the unused compensatory time at a rate of compensation not less than –

(a) The average regular rate received by such employee during the last 3 years of the employee's employment, or
(b) The final regular rate received by such employee, whichever is higher.

Before entering into an agreement for compensatory time in lieu of overtime, you would be wise to consult with your legal counsel to ensure that the agreement meets the requirements of the Fair Labor Standards Act.

****

CERTIFICATE OF ACHIEVEMENT FOR EXCELLENCE IN FINANCIAL REPORTING

MCRCSIP was awarded its 15th Certificate of Achievement for Excellence in Financial Reporting by the Governmental Financial Officers Association (GFOA) for its comprehensive annual financial report.

WORKPLACE SAFETY AWARENESS
"CLEANER CREATES POISONOUS GAS"

Mike Shultz
Director of Loss Control/Training

Last month, a motorcycle magazine, **"American Iron"**, wrote a "Safety Alert" article regarding a near fatal accident from misusing a brake cleaning product common to fleet and motorcycle repair shops. According to this article, an individual was nearly killed when he inhaled poisonous gas fumes when a small amount of the product was heated up during an aluminum TIG welding project. The individual indicated that he normally used a carburetor cleaner product to remove oil film from the aluminum surfaces prior to welding. In the absence of carburetor cleaner that day, he used a brake cleaning product.

As he began to perform his TIG welding operation, a minuscule amount of the brake cleaning product was heated up. As a result, he inhaled a small concentration of fumes/white smoke. That article goes on to say that he almost passed out but made it outside to some fresh air. Sometime later, his entire left side began shaking for about 10-15 minutes. He later discovered the following: ***"Vapors may decompose to harmful or fatal corrosive gases such as hydrogen chloride and possibly Phosgene".*** Phosgene is produced when the product vapors are exposed to argon gas and extreme heat. When TIG welding, argon gas and high temperatures was part of the process! He later discovered that concentrations of Phosgene, as little as 4 ppm (parts per million), or in his situation, the equivalency of a small puff of white smoke, can be very harmful and fatal. Exposure symptoms can be delayed from 6 to 48 hours and there is no antidote for Phosgene poisoning. If you survive, long-term health effects can occur, such as (but not limited to) chronic bronchitis, emphysema, kidney failure, pancreas damage, loss of coordination, speech, mental confusion, vertigo, low oxygen levels, scarred sinuses and damage to nasal nerve endings.

In the interest of workplace accident and injury prevention, MCRCSIP Loss Control continues to reinforce the importance of using chemical products properly when performing loss control visits and safety awareness training. We cannot overemphasize the need to take all necessary precautions to include reading container warning labels and the safety data sheets. Furthermore, chemicals should only be used as prescribed by the manufacturer and NEVER substitute one chemical for another! If you have questions regarding storage and usage, never hesitate to call the product manufacturer or your local supplier. Finally, when cleaning oil from aluminum before welding, contact your welding supplier.

The Lincoln Welding website suggests using a mild alkaline solution, like a strong soap, to remove oil or grease from aluminum. You may also use citrus-based degreasers, but be sure to rinse and dry the part before welding.

If you wish to read the entire "American Iron" article, please email Mike Shultz at mshultz@mcrcsip.org.

We wish to thank the Ionia County Road Commission for making us aware of this article.

MICHIGAN CATASTROPHIC CLAIMS ASSOCIATION ASSESSMENT

The Michigan Catastrophic Claims Association (MCCA) has increased its assessment to $186.00 per insured vehicle for the period July 1, 2013 to June 30, 2014. This assessment represents an increase of $11.00 (6%) from the current MCCA charge of $175.00.

We are required to pay the assessment to the MCCA to cover the cost of Personal Injury Protection (PIP) benefits guaranteed under Michigan's No-Fault insurance law.

SECURITY TIPS FOR THE MODERN INTERNET

Nick Wells
MCRCSIP IS Manager

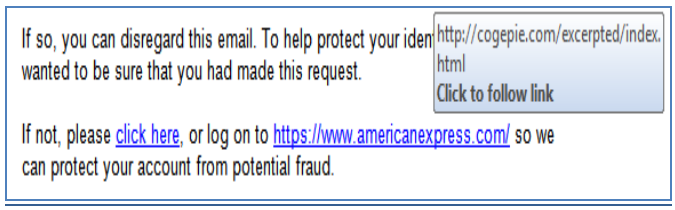
Lately, there've been a number of high-profile computer security events that could've easily been prevented had the people being hacked been a bit better educated. Here are four tips for reducing your chances of falling victim to such an attack

****

Don't Trust Email

Recently, the AP's twitter account was hacked and as a result, the Dow dipped for a little bit. This "hack" was possible because an AP staffer fell for a "phishing" attack and provided enough information to the attackers that they could gain access to the AP's twitter account. Phishing attacks usually start with an email to the target and rely on the target clicking a link then providing some information to a false website on the internet.

In the past, these emails were easy to spot due to poor spelling or grammar but these days, phishers have improved in that area. Lately, the best way to detect a phishing message is to "hover" (point at, but don't click) your mouse pointer over one of the links in the message and you should get a box similar to the one pictured below. In this box is the actual website you'll be taken to, not just the "name" of the link (the destination for "click here" is the same as the other link displayed).



We can see that the "name" of the link is "https://www.americanexpress.com/" but the actual destination in the pop-up box is "http://cogepie.com/excerpted/index.html".COGEPIE is a marine services provider that operates in the English channel, so there's not really a good reason for anyone to fill out any American Express forms on the cogiepie.com website. The form the phishers created looked like a legitimate American Express form, but because we hovered first, we could see this was a phishing attack (the Pool also doesn't use American Express which was another give away).

Email attachments are another reason to not trust your email. I tell everyone to delete any messages that come in with attachments that they weren't expecting. This was more of an issue before email filters started blocking attachments that run immediately, but it's still a good practice. Along with the previous advice, I also tell everyone to let the recipient know they're about to get a message with an attachment before sending the message. The idea is that eventually everyone will know when they're getting a good attachment so when they get an attachment they weren't expecting, they'll know it's safe to delete it.

Of course, email was never really designed with file transfers in mind, so not sending files via email attachments is a good idea. The alternative is to use something like an FTP server or a Cloud service such as Dropbox, Google Docs, Microsoft's SkyDrive, or Amazon's S3, however –

****

Don't Use Clouds (for now)

"The Cloud" has become so common that it's almost impossible to use a smartphone without interacting with someone's cloud in some fashion. If you don't use a smartphone, you might find that your email provider is using "The Cloud" for that now. If you just read the New York Times online, you're using the cloud. The reason for the sudden proliferation of cloud-based services is that, from a purely technical standpoint, clouds solve a lot of problems.

Basically, clouds are loosely associated groups of computers which are programmed to do the same thing. Because they're loosely associated, a single computer or several computers can go offline (either intentionally or due to failure) without affecting the services offered by the cloud. Data is also evenly distributed amongst computers in the cloud which means that it's always available. Additionally, clouds can be programmed to perform complex computations relatively quickly due to the large number of computers participating in the cloud.

What this means is that services hosted in the cloud such as email, websites, and databases are practically "always on" and files are almost never lost but it also gives IT teams managing the cloud computers the chance to perform critical maintenance without causing a service interruption. The problem though, is that according to the Electronic Communications Privacy Act of 1986, any data stored for more than 180 days in "online" storage is considered abandoned. This means that it would only require a subpoena to the storage host to acquire rather than a warrant.

It's tempting then to say, "ok, well I can put this file on my dropbox but delete it right away and then it won't be considered abandoned." Which is a reasonable thought, except that most cloud providers use a backup system that could keep your data around for much longer than 180 days, making it susceptible to subpoena. There is a bill which just passed the senate judiciary committee, Electronic Communications Privacy Act Amendments Act of 2013, which would require a probable cause warrant to access cloud data.

WWW.MCRCSIP.ORG

MCRCSIP'S
MEMBER ON-LINE START PAGE

The Pool's Member Start Page is your on-line access portal to the Pool. From the Start Page, you can submit a Proof of Loss form and use the new Physical Damage Claim form to submit claims.

You can also access an online copy of the EPL Guidelines and sample forms that you can download to your computer. The following chapters have been updated:

Chapter X	Wage & Hour Compliance
Chapter XI	Disability Discrimination
Chapter XII	FMLA Act
Chapter XIV	Open Meetings Act
Chapter XVI	Employee Privacy
Chapter XXII	Drugs & Alcohol

Member quarterly loss run reports are available on line but are only accessible to Member Managers.

Use a Strong Password

Typically, passwords are compromised when someone falls for a phishing attempt and just gives their password to a malicious user, but sometimes passwords are "guessed" which is why IT security people recommend "strong" passwords. The process of guessing a password typically involves a "Dictionary Attack" in which lists of words are tried sequentially, or when the target's personal information is assumed to make up all or part of the password. A strong password is one which will require so much of the attacker's time to guess that the attacker would sooner give up and move on to an easier target.

The first step towards a strong password starts with not using a word or phrase that's familiar to you, kids' names, favorite foods, your car, etc.; familiar numbers are also out, birthdates, anniversaries, and so on. You also need a fairly long password too, most passwords under 8 characters can be cracked in just a few minutes, try for 10 to 14 characters. How to come up with a 10 – 14 character password that isn't anything familiar can be difficult, but the trick is to use a mnemonic device to help you remember. For example, "whtttbsetamace" is a random string of 14 letters; well it just looks random, those letters happen to be the first letter of the first fourteen words of the second paragraph in the Declaration of Independence ("We hold these truths to be self-evident, that all men are created equal…").

That's a good start to a password, but it'll probably only take the computer sitting on your desk about twenty minutes to crack. You can add complexity by capitalizing some of the letters: "WhTtTbsEtamaCe" and you can buy another hour or two of cracking time. To further complicate the password, you can add numbers which would increase the password length or you can replace letters with numbers. A lot of people like to replace a letter with a number that looks like the letter, "WhTtTb5EtamaC3"; which works, you could also replace the letter with its position in the alphabet: "W8TtT25Et1maC3". Finally, you can add some punctuation marks and it'll take several days to crack with most computers available to attackers: "W*TtT25Et1ma#3".

You don't need to go too overboard with the complexity, the idea is to make the password complicated enough that the attacker gives up before they can guess it, but not so complicated that you can't remember it. You should also avoid using your password more than once; on Facebook, you login using either your phone number or your email address and a password which makes me curious how many people have the same password for Facebook as they do for their email. Another thing to watch out for is entering your passwords using a mobile device, whether a flip-phone style device, or a touch screen, it probably will slow you down enough that someone watching you will have an easy time reading your password.

****

Don't Use Wi-Fi for Anything Serious

Wi-Fi hotspots are easy for attackers to compromise. Since all of the Wi-Fi data is being broadcast from your computer to the access point and back over a well-known set of frequencies, anyone can record the transmissions. Most Wi-Fi access points now come with encryption turned on by default, but even still an attacker can obtain the encryption key within a few hours no matter how complex it is.

Wi-Fi encryption keys aren't obfuscated the same way passwords are because the other side needs the key to decode the Wi-Fi data. Passwords are "one-way" encrypted, which means they cannot be de-crypted to their original form, Wi-Fi keys are two-way encrypted and can be reverted to their original form. After enough Wi-Fi data has been recorded by an attacker, it's a simple matter of looking for repeating sequences in the encrypted data. De-crypting the most complex Wi-Fi keys takes only a few hours because most Wi-Fi access points use low strength ciphers.

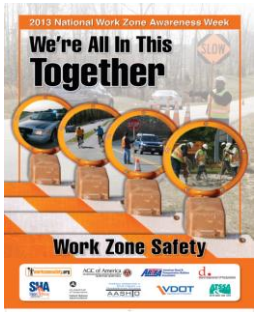
Once the Wi-Fi key has been obtained, an attacker can just sit back and record any data that's transmitted with very little effort. With a few more minutes of work, an attacker may be able to compromise any wired network connected to the hotspot. To mitigate this, you can access some websites using https (https://www.mcrcsip.org instead of http://www.mcrcsip.org) but that doesn't always work. A more secure method is to use a VPN which would encrypt any internet traffic and send it to a secure VPN server. VPN technologies also use two-way encryption but have stronger ciphers, so you'll want to use them briefly and sparingly as this reduces the attacker's data sample from which he can glean the encryption key

****

Use Your Head

As a final "tip", there are two undefeatable security devices that every computer has, the power switch and the user. You should know that the Internet is as amazing as it gets, but you should also know that it's very easy to end up in a bad place quickly. Just as in real life, the best way to get out of a bad spot is to recognize them before you get there and steer clear.

_____



2013 WORK ZONE SAFETY

Mike Shultz
MCRCSIP Director of Loss Control/Training

With winter weather finally leaving Michigan, MCRCSIP members are preparing for the 2013 Road Construction/Maintenance season. As part of the preparation process and throughout this season, we must always keep work zone safety in the forefront! Safety education, supervisory monitoring applies to (but not limited to):

- Road workers, including seasonal employees
- Member equipment positioning and visibility, including other specialty equipment
- Safety for the motoring public traveling thru/around our projects

Employees working in/near the roadway should never take short cuts or underestimate the many hazards associated with work zones. Particularly approaching work site traffic and heavy equipment and truck operations. Employees must always remain alert to changing conditions, look out for one another and follow their organizations' safety rules and procedures. Wearing high visibility attire (vests, jackets, etc.) has greatly improved over the past several years. Let's continue that positive trend by wearing your PPE when outside the vehicle cab!

Work Zone Awareness Training should be ongoing, whether 10 minutes or one full day. DVD's and in-house training presentations are available to all members by contacting the MCRCSIP Loss Control. Also, there are free training materials that can be downloaded from the Federal Highway Administration and American Road and Transportation Builders Association. Contact www.workzonesafety.org, The National Work Zone Safety Information Clearinghouse, for more information.

———

"PAIN AND SUFFERING" IS NOT BODILY INJURY

William L. Henn, Attorney

The Michigan Court of Appeals recently issued a published decision in which it concludes that governmental immunity bars recovery for "pain and suffering" and "shock and emotional damage" because those types of injuries are not physical bodily injuries.

The litigation in *Hunter v City of Flint Transportation Dep't* arose from an auto accident in which the plaintiff's vehicle was side-swiped by a dump truck owned by the defendant. The collision was low speed: the vehicles were traveling only approximately 10-15 mph at the time of the crash. Allegedly as a result of the impact, however, plaintiff was diagnosed with low back pain which he testified made it more difficult for him to lead his daily life. Approximately seven months after the accident, he sought additional medical care, complaining of neck and back pain, spasms, and weakness. He was diagnosed with bilateral sacroiliac joint inflammation, a herniated disc, and a pinched nerve.

Plaintiff alleged that as a result of the crash, he was unable to work, was unable to perform chores around his house, could not sit or stand for long periods of time, was unable to drive, bend, or lift more than 5-10 lbs., and could no longer play softball or basketball with his son and children that he mentored. He claimed to have experienced "shock and emotional damage," as well as "pain and suffering," as a consequence of these limitations,

The defendant moved for summary disposition, arguing that the motor vehicle exception to immunity does not permit a plaintiff to recover for "emotional damages" or so-called "pain and suffering." The trial court denied the defendant's motion, but an immediate appeal ensued.

The Court of Appeals reversed the trial court, and in so doing construed the plain language of the motor vehicle exception in light of the Supreme Court's decision in *Wesche v Mecosta Co Rd Comm*. Relying upon *Wesche*'s definition of the term "bodily injury" as "pertaining to the body" or "corporeal or material, as contrasted with spiritual or mental," the Court of Appeals in *Hunter* concluded that the plaintiff's claimed injuries for "pain and suffering" and "shock and emotional damage" were not physical damage to a person's body, and therefore were barred by governmental immunity.

Presumably, because the highway exception to immunity contains a similar "bodily injury" limitation, *Hunter's* reasoning will be equally applicable in that context. This may not be established without some time and effort, however. By analogy, after *Wesche* was decided, plaintiffs argued that its precedent was not applicable in the highway exception context, despite the nearly identical language employed in the two statutes. Also, because *Hunter* was very recently decided, it is unknown whether the plaintiff will pursue an appeal to the Michigan Supreme Court.

Michigan County Road Commission Self-Insurance Pool
417 Seymour Avenue, Suite #2
Lansing, Michigan 48933

The Pool Cue is published quarterly by the
Michigan County Road Commission
Self-Insurance Pool
417 Seymour Avenue, Suite #2
Lansing, Michigan 48933

Past and current issues of the Pool Cue are available on the MCRCSIP website – www.mcrcsip.org.