Leaderschoice INSURANCE SERVICES

June 2019 | Volume 9 | Issue 6

NEWSALERT

Business Continuity

Prepare for Possible PG&E Power Shutdowns

PG&E HAS warned California residents and businesses that it may shut down the power grid for as long as five days for large portions of the state when there are high-wind conditions during the dry fire season.

That's because PG&E's infrastructure was found to be the cause of several recent wildfires.

PG&E sent letters to customers informing them that "if extreme fire danger conditions threaten a portion of the electric system serving your community, it will be necessary for us to turn off electricity in the interest of public safety."

With the specter of multiple-day power outages, businesses need to be prepared for keeping their operations going and preventing losses that may not be covered by insurance.

Just think how difficult it would be if you lost access to your computers, which are the nervous system of any business today. If you have no power, your operations could be shuttered for all intents and purposes.

There a number of steps you can take to make sure your business is resilient and can keep functioning during power outages, especially if they last a few days:

Identify vital business functions

Identify business processes that will be affected by a power outage. These processes will differ from business to business, but once you put them all down on paper, it will be easier for you to make a plan to keep them going.

Create a continuity plan

Once you've identified those processes, you should brainstorm on how you can keep them going without your regular power supply.

Create a plan outlining how employees should respond to the power outage. Post emergency numbers on sight for employees to call, including your electricity supplier to get an estimate on when power may be restored.

Back-up power a must

Consider investing in a back-up generator that can keep the critical functions of your firm going during a power outage.

Generators need to be used with adequate ventilation to avoid risk of carbon monoxide poisoning. Never plug generators directly into power outlets. Never use a generator under wet conditions, and let it cool off before refueling.

Cloud storage and MiFi

If you have not done so, you should secure a means of paperless document and file storage on the cloud. If there is a power outage and an accompanying surge, you could quickly lose your data. Plan ahead with a cloud server.

You should also prepare a system of personal wireless hotspots, or MiFi devices, so that even when the internet goes down, you can finish important tasks requiring web access, such as setting up an e-mail auto-response.

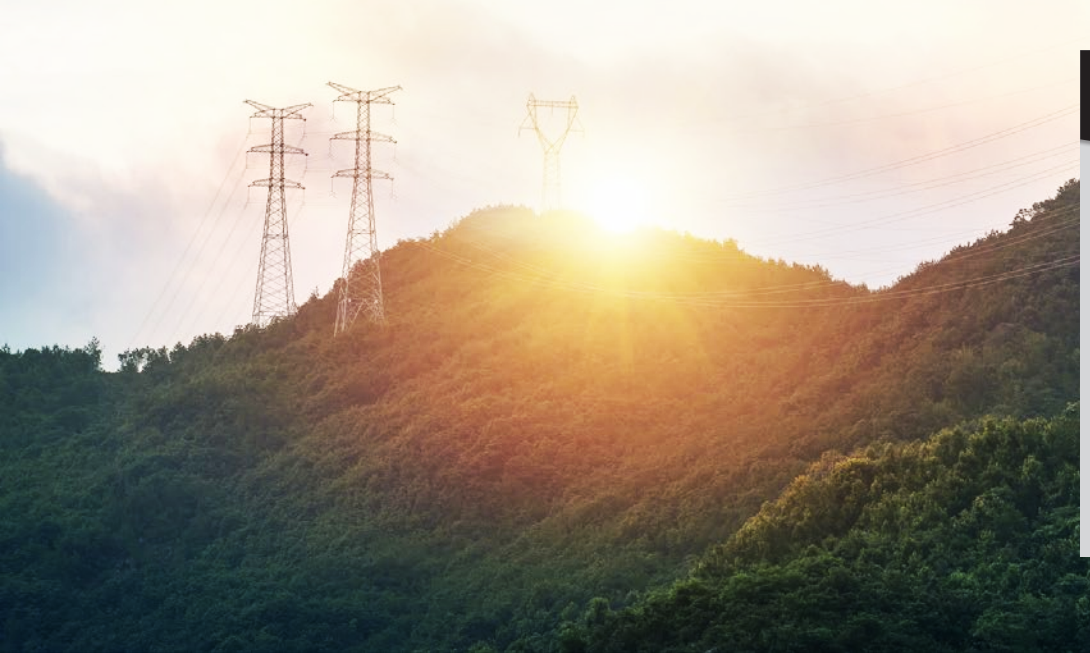
MAKE A SURVIVAL KIT

Create a kit with at least the following:

- Cash
- Medical supplies
- Extra gas
- Portable phone batteries for devices
- Water
- Canned food
- Flashlights
- Rope and other basic items.

Keep the kit in an easy-to-reach place.

See 'Interruption' on page 2



Leaderschoice INSURANCE SERVICES

CONTACT US

700 E Street
Sacramento, CA 95814

Phone: 866.211.2123
Fax: 866.913.7036
www.leaderschoiceins.com

License No. 0G80276

If you would like to receive this newsletter electronically, e-mail us at: info@leaderschoiceins.com

Workers' Comp

Construction Dual-Wage Changes Ahead

THE WORKERS' Compensation Insurance Rating Bureau of California will recommend dual-wage threshold changes to a number of construction classifications for the 2020 workers' compensation policy year.

The Rating Bureau will make the recommendations to the Department of Insurance during its annual rate filing in June. The recommendations would have to be approved by the state insurance commissioner.

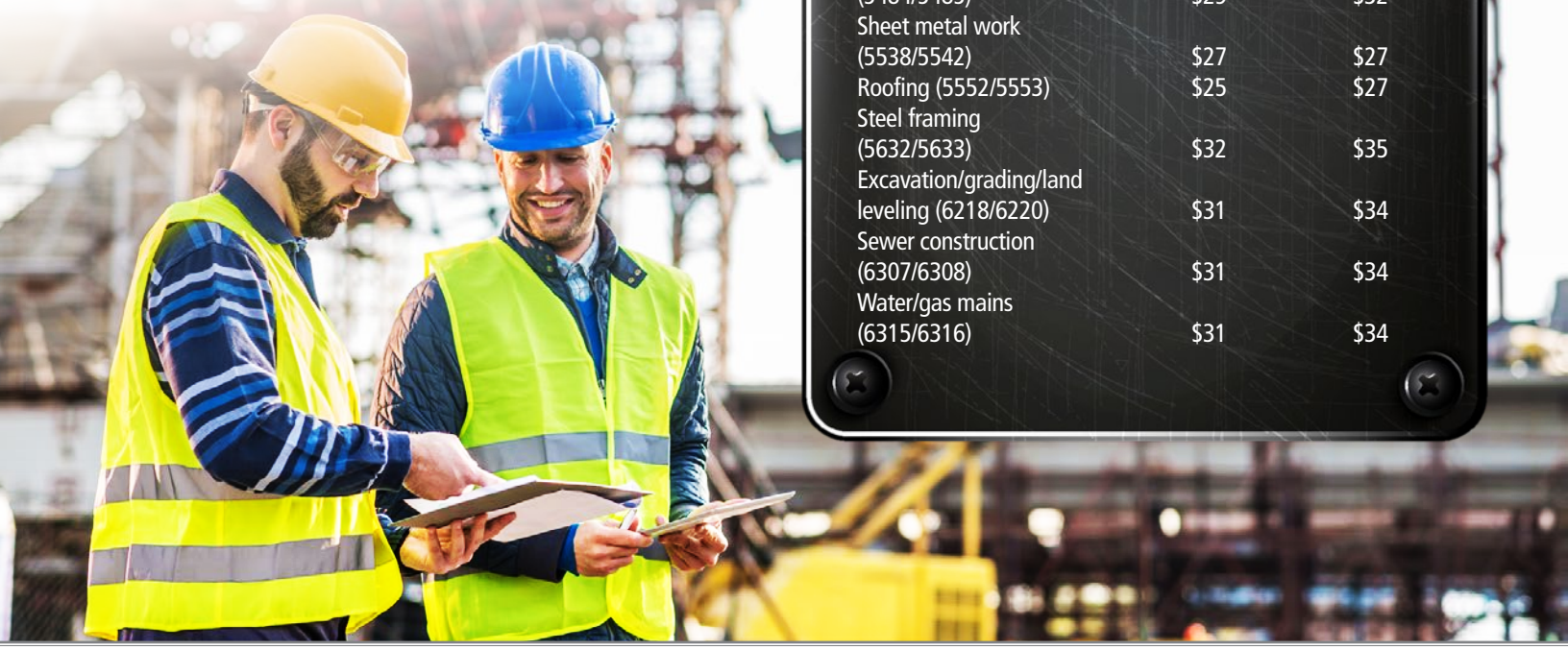
While most workers' compensation classes have one rate, in some classes the difference in claims costs between high- and lower-wage workers is so great that a dual-wage classification is needed. In those cases, the workers above the threshold rate are assigned one rate, while those below that threshold are assigned a higher rate. This is usually because the higher-wage workers are generally more experienced and tend to suffer fewer workplace injuries compared to those below the threshold.

There are 18 dual-wage classes, but not all of them are in line for changes.

Opposite is the list of changes the Rating Bureau plans to recommend in its rate filing. ❖

PROPOSED CHANGES

Class	Current	Proposed
Masonry (5027/28)	$27	$28
Electrical wiring (5190/5140)	$32	$32
Plumbing (5183/5187)	$26	$28
Automatic sprinkler installation (5185/5187)	$27	$29
Concrete cement work (5201/5205)	$25	$28
Carpentry (5403/5432)	$32	$35
Wallboard application (5446/5447)	$34	$36
Glaziers (5467/5470)	$32	$33
Painting/waterproofing (5474/5482)	$26	$28
Plaster or stucco work (5484/5485)	$29	$32
Sheet metal work (5538/5542)	$27	$27
Roofing (5552/5553)	$25	$27
Steel framing (5632/5633)	$32	$35
Excavation/grading/land leveling (6218/6220)	$31	$34
Sewer construction (6307/6308)	$31	$34
Water/gas mains (6315/6316)	$31	$34



Continued from page 1

Business Interruption Coverage Can Cover Lost Income

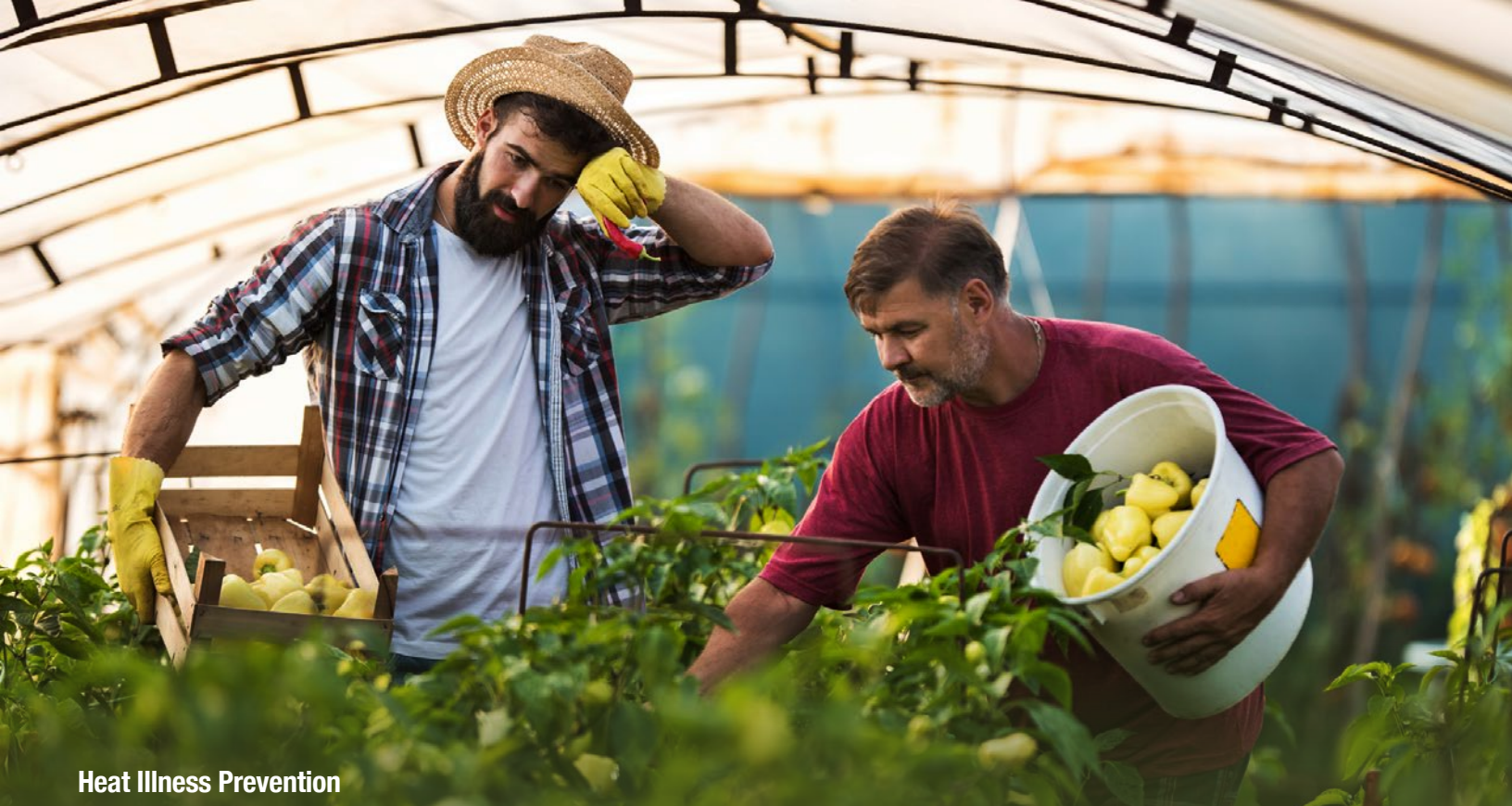
Consider business interruption coverage

The best way to minimize the financial blow is to have the proper insurance in place.

A multiple-day power outage could really crimp your income stream and, if you lose money due to your inability to operate, the typical business owner's policy won't cover lost revenue.

But, a business interruption policy would. These policies will reimburse you for lost revenues due to a number of events, including "service interruption" due to power outages and other utility services interruptions.

The important caveat is that the interruption was not caused by any of your own faulty equipment or wiring. But if the power company is shutting down power, any losses you incur should be a valid claim. ❖



Heat Illness Prevention

Worker Behavior, Habits Can Thwart Safety Efforts

EVERY SUMMER thousands of American workers suffer from heat illness after working in hot conditions and not taking the necessary precautions to protect themselves.

Even if employers follow the letter of Cal/OSHA heat illness prevention regulations, the human factor can often thwart those efforts. The biggest challenge in implementing a heat illness prevention program is cutting through misconceptions about heat illness and workers not understanding how to identify the initial signs of such illness.

You also have to make sure that your supervisors are all on board in protecting your workers. Just one bad supervisor who doesn't allow an outdoor employee to take a rest or water break can put that person's life at risk. Here are some problems that you may encounter when instituting a heat illness prevention policy for your staff, and how to deal with them:

Underestimating the risk

Many outdoor workers will plow through, even when they feel discomfort, thirst and symptoms of heat stroke. This machismo can quickly lead to trouble.

Unfortunately, heat illness symptoms can be subtle and easily misinterpreted as something small. For example, a worker may get a heat rash or cramps and dismiss them as just the result of hard work, when they should instead take a rest break in a shaded area and drink fluids – water or a sports drink is best.

Subtle heat illness symptoms include:

- Thirst
- Heavy sweating
- Headache
- Nausea
- Dizziness
- Irritability

Action: When the mercury exceeds 80 degrees, make rest and shade breaks mandatory.

Under Cal/OSHA guidelines, employers must provide access to shade and encourage employees to take a cool-down rest in the shade for at least five minutes every hour. Also, every workday should start with reminders about the symptoms of heat stress. Consider instituting a buddy system, as well.

Not drinking enough water

The most common way outdoor workers develop heat illness is by not drinking enough fluids.

When they get dehydrated their concentration can wane, leading to mistakes that cause accidents and injuries. Many employees may think they need to drink water or a sports drink only when they feel thirsty. Or maybe they reach for a Coca-Cola or Mountain Dew instead of water.

Action: Provide enough fresh water so that each employee can drink at least 1 quart, or four 8 ounce glasses, of water per hour, and encourage them to do so. It should be readily available and accessible. Provide reusable water, so they can keep their own water close at hand. Supervisors must enforce breaks on the hour, during which employees should rehydrate.

Newbies

With the expanding economy, employers have to hire more inexperienced workers. And with inexperience working in the heat comes the potential for danger, since the new workers may not recognize heat illness symptoms and the need for regular water and rest breaks.

Action: Pair new workers up with experienced ones, and do not let them start working without an introduction to heat illness prevention and the importance of following your safety rules. ❖

Cyber Security

The Risks of Staff Using Personal Devices for Work

AS MORE employees use their personal mobile devices for work, companies are being forced to confront the resulting security implications as well as how the devices are changing behaviors in the workplace.

Many businesses have responded by implementing policies to establish parameters.

The biggest risk to the company is hacking, cyber attacks and lost devices that may allow outsiders to gain access to the company database and e-mail.

This trend is generally referred to as "Bring Your Own Device," or BYOD. Some companies even allow employees to replace their work laptop computer with their own personal PC, which is sometimes referred to as BYOC. Here's what you should focus on:

Data risks

A report by law firm Littler Mendelson looked at five information security threats posed by BYODs:

Lost or stolen devices – According to a study by the Ponemon Institute, 39% of respondents reported that their organizations had sustained a data security breach as a result of lost or stolen equipment. Put simply, if your employees use their personal mobile devices for work, your company data is at risk if they lose their gadget.

Malware – Malicious software created for mobile devices has exploded. Malware can help hackers gain access to your company data.

Friends and family – A family member, friend or acquaintance can gain access to the device and cause problems.

Links to the cloud – Most apps allow users to store their documents and data using cloud-based storage, the report states. Employers must evaluate whether the sites provide sufficient security if the employee plans to store company information using the apps.

Security breaches – If you have a breach in security, it could expose your company to government enforcement actions, civil penalties and litigation. You could also be sued if the breach exposed personally identifiable information of employees or customers. There are also contractual obligations, which increasingly are including responsibilities to safeguard against data breaches.

Behavior issues

"The National Business Ethics Survey" by the Ethics Resource Center found that active social networkers are likely to believe that certain questionable behaviors are acceptable, such as:

- Blogging or tweeting negatively about your company or colleagues.
- Keeping a copy of confidential work documents in case they need them in their next jobs.
- Taking a copy of work software home for use on their personal computers.

Also, wage and hour implications can arise from using a mobile device to conduct work while off the clock. You should not require your staff to deal with work issues on their mobile devices during non-working hours. ❖

WHAT YOU CAN DO

Littler Mendelson recommends:

- Deciding which employees should be permitted to participate in a BYOD program. You may want to exclude senior executives whose data is more likely to be relevant in litigation, research and development employees and sales staff, who may store client information on their devices.
- Creating policies that address off-the-clock work.
- Informing staff that if they use their own device the company must be authorized to access their devices for record retention or litigation holds or investigations.
- Obtaining employees' written consent to monitor the BYOD device, remotely wipe the device if needed, install security software and copy data if necessary.
- Following good security practices.
- Barring employees' friends or family from using the devices.
- Creating a policy limiting the use of cloud-based storage.