

## WORKERS' COMP

### Agency to File for 3.4% Rate Increase for 2015

**T**HE STATE'S workers' compensation rating agency is preparing to file for a 2015 benchmark rate increase that is about 3.4% above the rates approved for this year.

The Workers' Compensation Insurance Rating Bureau noted after examining industry data and trends that treatment costs for injured workers continue climbing and that claims are being filed with increasing frequency.

The recommended benchmark rate is also 7.9% above the pure premium rates that insurers had on file as of June this year.

The Rating Bureau could amend the filing in late September after it receives more data on claims costs through July of this year.

The new average benchmark rate level, across all class codes in California, should be \$2.77 per \$100 of payroll effective January 1, 2015, according to the Rating Bureau.

That's compared with the \$2.57 average insurers had on file as of July 1, and with the average advisory pure premium rate of \$2.68 as of Jan. 1, 2014.

The insurance commissioner has the final say on benchmark rates, but insurers are free to price as they please, using the benchmarks as guideposts.

Benchmark rates cover just the cost of claims and administering them and don't include insurers' other overhead costs.

In a cover letter accompanying the filing, the Rating Bureau cited a number of factors contributing to the proposed increase, including:

- Continued adverse medical loss development.

- Greater recognition of changing long-term medical paid-loss development patterns.

- Continued high levels of indemnity claim frequency.

- Claims-adjusting expenses that are higher than anticipated, in part attributable to lower-than-projected frictional cost savings resulting from the latest workers' comp reform legislation, SB 863, which was passed in 2012 and took effect in 2013.

- Wage growth that is lower than forecast.

#### Claims frequency varies by region

A new report by the Rating Bureau, "State of the California Workers' Compensation Insurance System," released in August 2014, indicates that geography also plays a part in claims, which plays out in the final prices that employers pay.

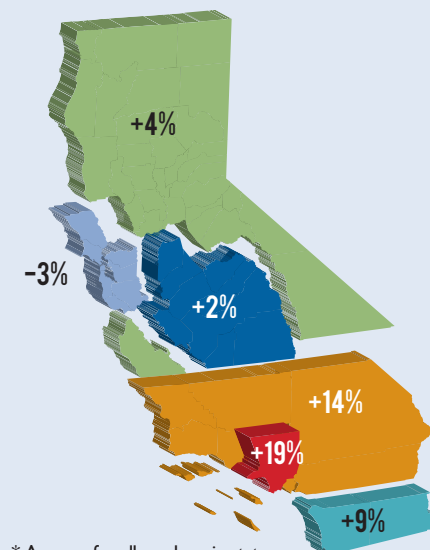
The report notes that overall, the number of indemnity claims (those that include payments to workers for lost time at work) has steadily increased over the last few years, largely driven by inordinate growth in claims numbers in Southern California.

In the last three years, the number of indemnity claims has increased by 19% in Los Angeles County, 14% in the Los Angeles Basin and 9% in San Diego, according to the Rating Bureau (see chart to the right).

"The frequency of permanent partial disability claims – including those involving cumulative injuries or multiple injured body parts – has increased sharply in the Los Angeles area," the Rating Bureau's report says. ❖

#### Claims Frequency up 9%\*

Claims frequency (the number of claims filed per 100 workers) varies wildly in the state.



\* Average for all workers in state.  
Source: Workers' Compensation Insurance Rating Bureau

## CONTACT US

#### Gilroy Office

9015 Murray Ave #110  
Gilroy, CA 95020  
Phone: 408-842-2131

#### Pleasant Hill Office

200 Gregory Lane, Bldg A  
Pleasant Hill, CA 94523  
Phone: 925-686-2860

#### Los Gatos Office

20 S. Santa Cruz Ave Ste. 319  
Los Gatos, CA 95030  
Phone: 408-354-7711

License No. 0504035

## CYBER THREAT

# Hackers Can Tap USB Devices in New Attacks

**N**EW RESEARCH says that USB devices like thumb drives, and even keyboards and mice, pose one of the biggest cyber threats to enterprises.

Two scientists and researchers with Berlin's SR Labs presented on the newest cyber threat at the recent "Black Hat" hacking conference in Las Vegas in a presentation titled: "Bad USB – On Accessories that Turn Evil."

Malicious code can creep into these devices through malware on a computer and be used to hack both personal and business computers, according to SR Labs. Karsten Nohl, chief scientist at the German company, said that hackers or malware can load malicious software onto the computer chips that control the functions of USB devices, which typically don't have any protection against tampering with their code.

Even more disconcerting is the fact that it's virtually impossible to tell from where the virus originated.

SR Labs is known for uncovering major flaws in mobile phone technology. Its new research indicates just how easy it is for hackers to exploit weaknesses in simple devices in order to do serious damage to a computer or network.

SR Labs has performed attacks by writing malicious code onto USB control chips used in thumb drives and smart phones. Once the USB device is attached to a computer, the malicious software can log keystrokes, spy on communications and destroy data, he said.

A USB device that appears completely empty can still contain malware, even when formatted.

Interestingly, the computer to which the infected USB device is attached does not detect the virus because anti-virus programs only scan software written into a computer or a device's memory. However, these viruses can be implanted in the "firmware" which controls the device's functions, and anti-virus programs do not scan firmware.

SR Labs, when running its tests, was able to gain remote access to a computer by having the USB instruct the computer to download a malicious program with instructions that the PC believed were coming from a keyboard. The virus in the USB device was also able to change DNS network settings on a computer, instructing it to route all of its

Internet traffic through malicious servers.

Once a computer is infected, it could be programmed to infect all USB devices that are subsequently attached to it, which would then in turn corrupt machines that they contact. In other words, if one tainted USB device is inserted into a workplace computer attached to a network, it can infect all USB devices in your workplace.

"It becomes self-propagating and extremely persistent," Nohl said in a prepared statement. "You can never remove it."

In one demonstration shown at the "Black Hat" conference, a standard USB drive was inserted into a normal computer. Malicious code implanted on the stick tricked the machine into thinking a keyboard had been plugged in.

After just a few moments, the "keyboard" began typing in commands – and instructed the computer to download a malicious program from the Internet.

Another demo involved a Samsung smart phone. When plugged in to charge, the phone would trick the computer into thinking it was in fact a network card. It meant that when the user accessed the Internet, their browsing was secretly hijacked.

Nohl demonstrated how they were able to create a fake copy of PayPal's website, and steal user log-in details as a result.

Unlike other similar attacks, where simply looking at the Web address can give away a scam website, there were no visible clues that a user was under threat.

### The takeaway

USB is ubiquitous across all devices, and all desktop and laptops have at least two and often more than four USB outlets for plugging in keyboards, mice, peripherals like printers and scanners, mobile phones, tablets and USB devices.

If you have not already done so, you should have a policy prohibiting your staff from plugging in USB devices that were not issued to them at work. In fact, you may want to consider even prohibiting your staff from using company-issued USB devices such as memory sticks or mobile phones. ❖



## DIFFERENCE IN CONDITIONS

# Is Your Business Covered for an Earthquake Claim?

**T**HE EARTHQUAKE in Napa last month illustrates the exposure that all businesses in the Golden State have to this unpredictable risk.

While most modern structures are built to withstand earthquakes of a certain size, many older buildings throughout the state are not up to standard, resulting in more damage and replacement costs should a temblor strike. The reality is that whatever its age, a building could suffer structural damage that could cost millions to repair.

Besides the risk to people and property, many business owners are unfortunately surprised to learn after the fact that their commercial property policy won't cover damage from an earthquake.

Insurers set rates so that the premium they collect on policies will cover any money expected to be paid out in claims. The company spreads the risk of loss over many policies in the hope that only a small number will suffer damage.

However, large disasters, like floods and earthquake, will typically affect many policyholders at once, a scenario that many insurers try to avoid – and they do so often by excluding such coverage in their commercial policies.

To fill this gap, you can turn to a “Differences in Conditions” policy. A DIC policy can be useful if you face either flood or earthquake risk in your area and your property carrier doesn't offer coverage for these risks, cannot provide full limits to cover potential losses, or can only offer this coverage at rates that are essentially cost-prohibitive.

Most property policies are written on an “open perils” basis (meaning they will cover many types of claims resulting from acts of God), but they usually exclude flood and earthquake risk.

Besides providing coverage for flood and earthquake losses, a DIC policy may also be used to provide excess limits over flood and earthquake coverages made available by endorsements to a commercial property policy or through the National Flood Insurance Program.

Furthermore, because a DIC is often written as a type of inland marine insurance, it also may be used to address other risks that may not be covered in commercial property policies, such as property in transit, property overseas, or business interruption claims arising from an earthquake or transit loss.

One thing you should know, however, is that a DIC policy is what's known as a “non-filed” policy.

That means insurers do not have to file rates for approval with state insurance departments, and they have greater flexibility in setting rates and drafting policy language. Insurers are often willing to negotiate coverages and limits with policyholders.

Often, the terms and conditions in a DIC policy can vary in important ways from one insurer to the next, so you need to choose carefully.

Opting for a DIC policy with terms and definitions that conflict with your underlying commercial property insurance policy can cause coverage problems.

### Does your business need a DIC policy?

The first thing you should ask yourself is if you need more protection than that provided by standard property insurance, especially with regard to flood and earthquake perils.

It's most likely that your policy won't provide any protection for these risks.

If you live in a region that is prone to earthquakes and your commercial property policy excludes such events, you may need a DIC policy.

This holds true especially for contractors, manufacturers, retailers, and a variety of service and professional businesses. You may also need it if you carry inventory that can be damaged during an quake or if you own your building.

Since flood or earthquake losses can be catastrophic, no one insurer may be willing to write a DIC policy with the limits you request or require.

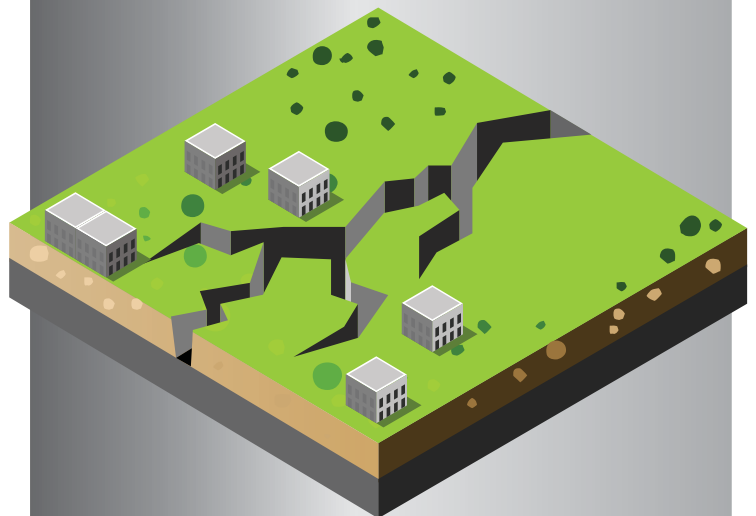
In such cases, two or more insurers may be willing to share the risk on a layered basis or through a quota share (an agreed-on percentage) approach.

We are here to help you by comparing the coverages and exclusions of various DIC policies to find which one would best fit your business's needs. ❖

## What a DIC Covers

THE TYPICAL commercial DIC policy can provide earthquake and/or flood coverage for:

- Buildings.
- Tenant improvements and betterments.
- Business personal property and/or stock.
- Loss of business income, rental income or if you incur extra expenses.



**We can help you decide whether a policy is right for you. Call us today!**



## EMPLOYEE ISSUES

# The Triple Regulatory and Litigation Threat

**W**ITH HEAVY fines and the threat of lawsuits hanging over their heads, employers already know they have to walk a fine line when managing their employees.

But in the last four years, thanks to increased regulatory action as well as new regulations and laws, there's been a serious uptick in litigation and enforcement in three areas: wage and hour litigation, family medical and disability leave and labor and recruitment.

### 1. Wage and hour litigation

During the past half decade, there has been a surge in wage and hour litigation. Much to the dismay of business owners, their employees - with help from their attorneys - have had great success in suing and winning large lawsuits against all types of companies of all sizes in a plethora of industries.

With more complaints landing on its doorstep, the Wage and Hour Division of the U.S. Department of Labor in 2013 requested a budget increase of \$6.4 million to support the addition of 57 investigators to enforce a variety of laws.

The Labor Department has also been very successful in securing settlements from employers. In fiscal year 2011, the DOL recovered \$225 million in back-wages for employees, up 28% from fiscal year 2010, and the largest amount collected in a single year in the division's history.

With the stakes high, your HR manager needs to be regularly reviewing company policies, procedures as well as actions to head potential litigation off at the pass.

If they identify an area where an employee may have been shorted, it's your duty to acknowledge the mistake and rectify it by making them whole.

### 2. Workers want their time off

The Americans with Disabilities Act, the Family Medical and Leave Act, and other state and federal leave laws have very specific rules for employees to take time off for illnesses, vacations, taking care of sick family members, and more.

And recently both laws have been greatly expanded to include more protected classes for disabilities and more reasons employees can take time off from work to care for family members.

While the laws are usually quite straightforward, employees continue suing their employers in record numbers.

Your HR manager should make sure that your paid time off and disability and family leave policies are in sync with both federal and California laws.

### 3. EEOC and NLRB on the prowl

The Equal Employment Opportunity Commission has been stringently enforcing its "Strategic Enforcement Plan," which focuses on six areas of priority:

- Eliminating barriers in recruitment and hiring
- Protecting immigrant, migrant and other vulnerable workers

- Addressing emerging and developing issues
- Enforcing equal pay laws
- Preserving access to the legal system
- Preventing harassment in the workplace

Also, you may know the National Labor Relations Board for its protection of union rights and rights of employees to unionize. But during the last few years, with the advent of social media and its accompanying employee vs. employer rants on social media, the NLRB has also been aggressively cracking down on employers who restrict their employee's right to free speech.

While limiting what your employees post about the company may help your business from a public relations standpoint, it can also create new legal problems.

The NLRB has issued guidance on numerous occasions on at what point employers cross the line when they try to curtail commentary by employers on their social media pages.

All of these issues are major pitfalls for employers.

To avoid falling into the litigation or regulatory trap, you should review and update your employee handbook regularly and consult with a legal professional to ensure that your company policies are in compliance with state and federal law. ❖



**Insurance can cover costs associated with lawsuits stemming from these issues. We can find the right coverage for you. Call us today!**