HEFFERNAN INSURANCE BROKERS
Because You're Different
News You Can Use
November 2018 | Volume 6 | Issue 11

Sexual Harassment

Raft of New Laws Puts Pressure on Employers

CALIFORNIA GOV. Jerry Brown has signed into law a number of bills that will drastically change the landscape for employers trying to resolve sexual harassment and discrimination claims.

Brown signed three bills that will make it easier for workers to bring claims of harassment and discrimination in the workplace, and curtail the ability of employers to resolve the claims with motions for summary judgment.

They will also prohibit non-disclosure agreements, and will expand the number of employers that will be required to provide anti-sexual-harassment training to their staff.

As an employer you need to be aware of the new laws to avoid future legal quagmires, as failing to comply with some of these laws could drastically increase an employer's liability.

Here's a rundown of what you need to know:

SB 1343

Existing law requires that organizations with 50 or more employees provide two hours of sexual-harassment prevention training to supervisors every two years. This was mandated two years ago under another piece of legislation, AB 1825.

The new law, which takes effect Jan 1, 2020, expands this training requirement to all employers in California with five or more employees.

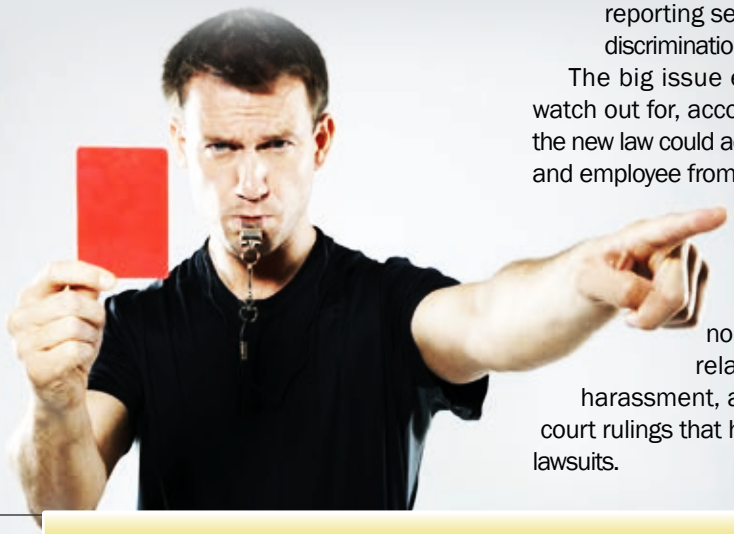
But SB 1343 goes beyond current law by requiring that all employees are trained every two years.

SB 820

This law takes effect Jan. 1, 2019 and will bar California employers from entering into settlement agreements that prevent the disclosure of information regarding:

- Acts of sexual assault;
- Acts of sexual harassment;
- Acts of workplace sexual harassment;
- Acts of workplace sex discrimination;
- The failure to prevent acts of workplace sexual harassment or sex discrimination; and
- Retaliation against a person for reporting sexual harassment or sex discrimination.

The big issue employers will need to watch out for, according to experts, is that the new law could actually keep the employer and employee from reaching resolutions for disputes.



SB 1300

This new law bars other non-disclosure agreements related to claims of sexual harassment, and also overturns prior court rulings that have limited harassment lawsuits.

SB 1300 bars employers from requiring an employee to sign a release of a Fair Employment and Housing Act claim or signing a non-disparagement or non-disclosure agreement related to unlawful acts in the workplace, including sexual harassment in exchange for a raise or bonus, or as a condition of employment or continued employment.

This law also takes effect Jan. 1, 2019.

One good thing, the prohibition does not apply a "negotiated settlement agreement to resolve an underlying claim under [FEHA]."

The new law will also make it more difficult to collect attorneys' fees and costs. Now they will only be granted if the court finds that the action was "frivolous, unreasonable, or totally without foundation when brought or the plaintiff continued to litigate after it clearly became so."

SB 1300 also expands current law under which an employer can be held responsible for sexual harassment committed by non-employees like clients, vendors and other third parties, if the employer knew or should have known of the conduct and failed to take

See 'Responsible' on page 2

Contact Us

HEFFERNAN INSURANCE BROKERS

If you have any questions regarding your coverage or our products, please call us at one of our offices:

Walnut Creek
San Francisco
Menlo Park
Portland
St. Louis
Petaluma
Los Angeles
Orange County
New York

Sales: 877-731-7905
Service: 800-234-6787

Risk Management

Your Firm May Need Professional Liability Coverage

MANY COMPANIES are leaving themselves exposed in one key area as they take on high-end professional services work.

As more work is intangible, many firms are missing a critical element of protection for their professional services.

Professional liability insurance in the past was mainly purchased by architects, accountants and lawyers, but with more work like coding, programing and other ventures spawned by technology, the need for this type of protection has grown.

In fact, a recent report by Forbes Insights and The Hanover found that 40% of small business owners believe they face professional risks, yet they have not purchased professional liability coverage as part of their overall insurance package.

Many more firms are in the business of consulting or providing hi-tech services. In addition, the rampant growth of social media has also fueled the need for this type of coverage.

Professional liability insurance, also called errors and omissions insurance (E&O insurance), protects your firm if you are sued for negligently performing your services.

BUSINESSES THAT NEED COVERAGE

- Technology and software firms
- Health and beauty services
- Therapists
- Architects
- Engineers
- Real estate agencies
- Consultants
- Marketing/ advertising firms
- Medical professionals
- Wedding and event planners

Coverage gaps

If you are relying solely on a general liability policy, it may not cover you in the event of a lawsuit over an issue with the services that you have rendered.

Professional liability coverage can be especially important if you have customers who sue you for non-performance of your products or services, or withhold payment due to a contract dispute.

What it covers

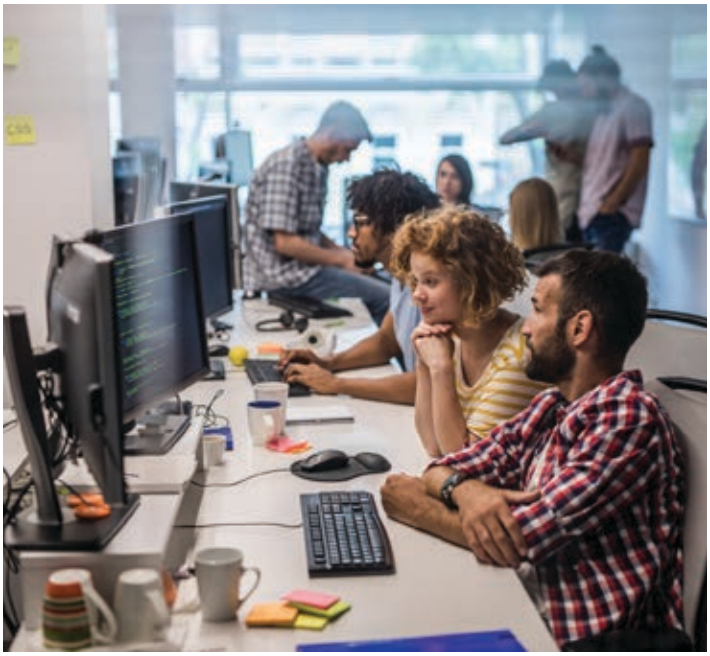
Negligence – Professional liability insurance coverage can protect you and your business against actual or alleged errors and omissions that may occur while providing your professional services.

These claims can include anything from giving incorrect advice or omitting a piece of information, to failing to deliver your service within a desired timeframe.

Legal costs – The policy includes covering your legal costs in defending against a claim. Some insurers will even appoint an attorney to represent you. ❖

WHEN COVERAGE WOULD KICK IN

- A marketing consultant develops a drip e-mail campaign for a retailer that doesn't generate the number of leads expected.
- A management consultant develops an organizational strategy to improve communications in a company, but problems persist at the client and communications don't improve.
- A software developer fails to develop an app to the client's specifications.



Continued from page 1

You Can Be Held Responsible for Harassment by Third Parties

immediate and appropriate corrective action.

Now employers can be held responsible for all forms of unlawful harassment committed by non-employees, not just sexual harassment.

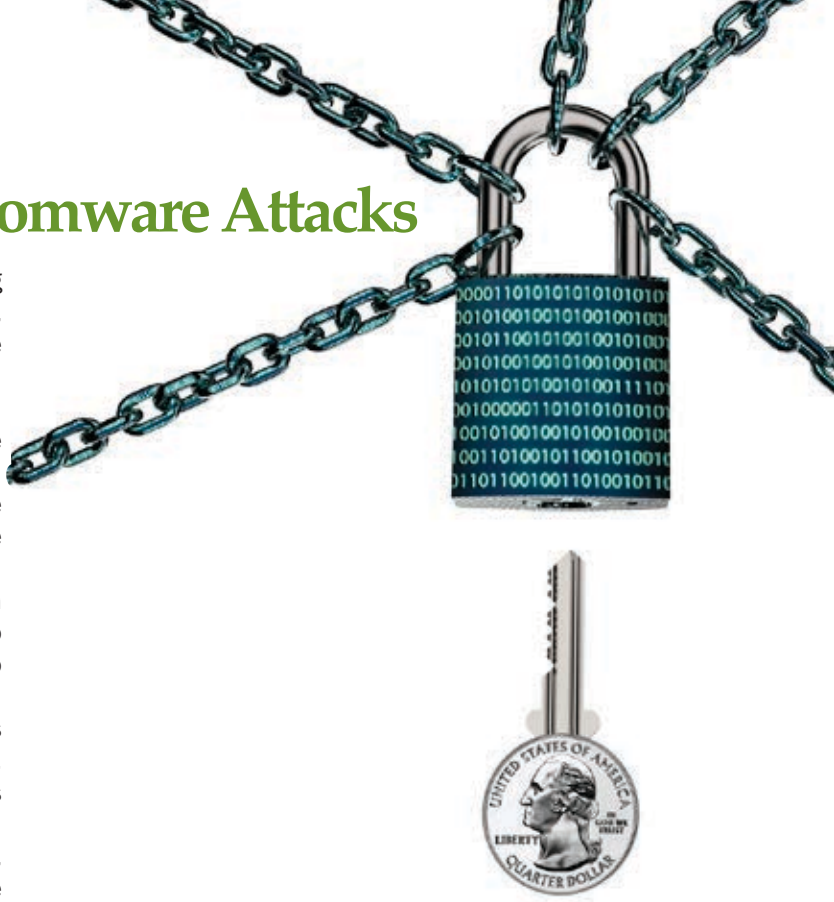
The law also includes an unusual section on "legislative intent," which is language that was designed as guidance for the courts but is not legally binding. It includes:

Single incident grounds for a claim – The new law declares that a "single incident of harassing conduct is sufficient to create a triable issue regarding the existence of a hostile work environment."

Stray remarks doctrine – Even a single discriminatory remark, even if not made directly in the context of an employment decision or uttered by a non-decision-maker, may be relevant and circumstantial evidence of discrimination.

Summary judgments – Harassment claims are "rarely appropriate for summary judgment." According to the law, summary judgment is a motion usually filed by the defendant to have the case thrown out before trial. ❖

Finding Coverage for Ransomware Attacks



IT'S A NIGHTMARE scenario for business owners. Employees log in to their workstations and attempt to access the usual systems, expecting to find customer reports. Instead, they find a message demanding money.

If the business wants to regain access to its software and data, it will have to pay a ransom. Until then, it is locked out. The business has become the latest victim of ransomware.

Ransomware is malicious software that hackers introduce into an organization's computer network to encrypt its data. The hackers hold the data hostage until their demands are met.

Those demands are normally for money, often payable in a crypto-currency such as Bitcoin. The hackers threaten to encrypt the data indefinitely, or even start deleting it, if they do not receive payment.

Ransomware has been around for a decade, but its use has exploded since 2015. Because it was infrequent until recently, insurance coverage for losses resulting from these attacks has not yet been widely purchased.

While cyber insurance has been available for several years, the coverages continue to evolve with the threats they insure against. Also, businesses have been slow to see a need for these policies, resulting in a low level of sales.

Consequently, an organization that falls victim to a ransomware attack might find itself uninsured. However, there are two potential avenues for coverage that many organizations already have – directors and officers (D&O) liability insurance and crime insurance.

Kidnap & ransom coverage

These types of policy often provide kidnap and ransom (K&R) coverage. This coverage, frequently purchased by multinational corporations, applies to an organization's cost to pay ransoms.

Traditionally, coverage applied only if an "insured person" such as an employee or executive was kidnapped. Such policies would do nothing for the victims of ransomware attacks.

Some insurers are now providing – either deliberately or unintentionally – K&R coverage that applies to ransoms paid in response to cyber extortion. Among the events that these policies may consider cyber extortion are:

- Threats to poison a computer system with malware.
- Threats to change, damage or destroy programs or data stored on a system if the owner does not pay a ransom.

Some insurers who provide K&R coverage did not anticipate covering ransomware losses and have made changes to the policies they sell. For example, some have added deductibles to the coverage, mirroring the terms of cyber policies, while others have capped the amount of business interruption coverage they will provide for cyber extortion losses.

Other insurers have changed their policies to better cover ransomware losses. Some have set up Bitcoin accounts for clients so that ransom payments can be made faster, shortening the length of time a business is incapacitated.

The takeaway

Experts expect the problem to become more urgent. The cost of global ransomware attacks in 2015 was $325 million, but by 2019 it is expected to be more than $11.5 billion.

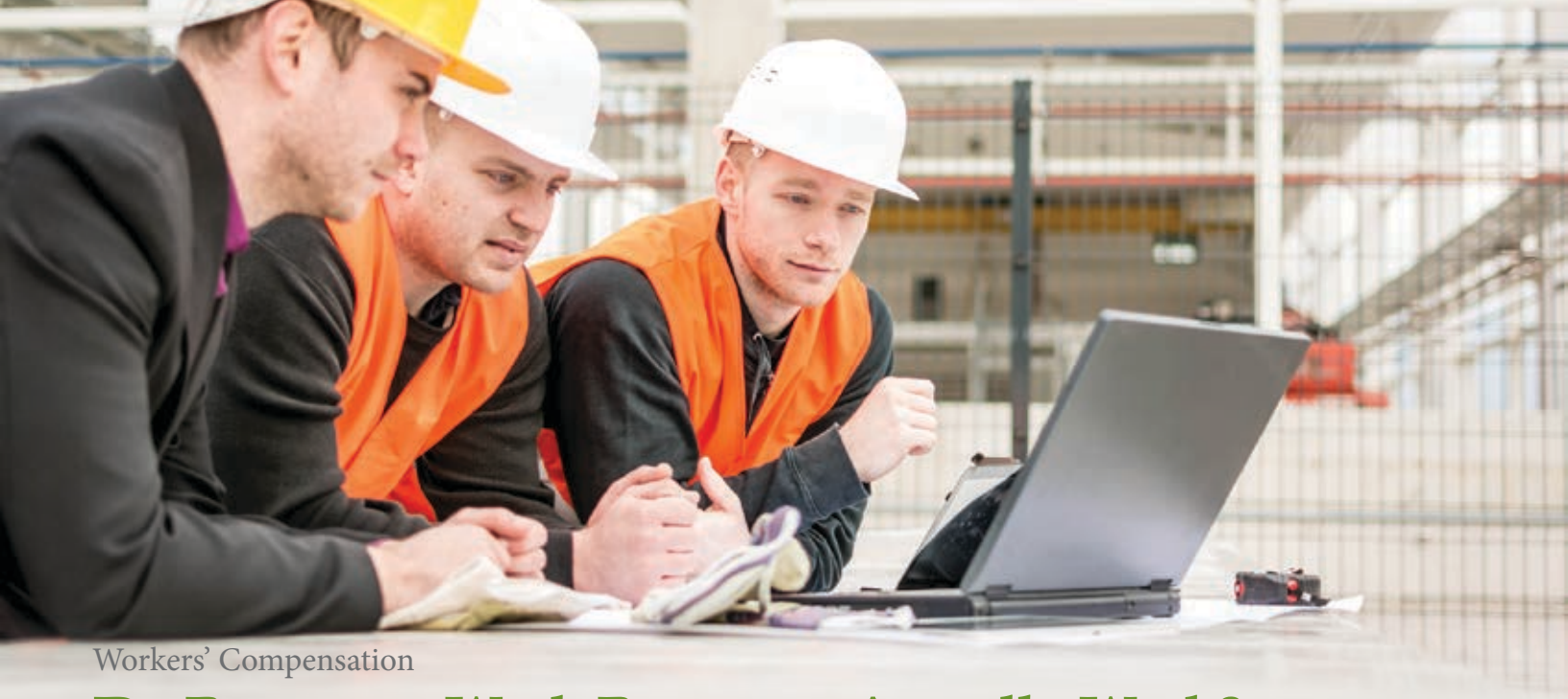
As the threat increases, organizations will have no choice but to insure against these losses, either through D&O coverage or cyber insurance.

Those who do not carry cyber insurance should review their D&O policies with their agents to determine whether the K&R coverage applies to ransomware losses.

If the coverage is missing, steps should be taken to obtain it, either through K&R coverage or cyber policies.

Cyber criminals are using ever more sophisticated tools. Sound network security practices are the best way to avoid disaster, but proper insurance coverage is essential if things should go wrong. ❖

WORRIED ABOUT RANSOMWARE AND COVERAGE?
CALL US: 877-731-7905



Workers' Compensation

Do Return-to-Work Programs Actually Work?

EMPLOYERS WHO have an injured worker are caught in a bind. As the worker recovers, they are faced with a decision of whether to settle the workers' comp claim and wait for the worker to fully heal, or bring them back in a lighter-duty assignment unlikely to aggravate the injury.

Each, of course, has long-term consequences.

If you settle too many claims, your workers' comp premiums are likely to go up.

Similarly, letting the worker stay home until fully healed means you may be missing their valuable experience. Secondly, your workers' comp policy is still paying out lost wage benefits for as long as that worker stays home.

The long-term consequences of not having the worker come back to the workforce, even in a reduced capacity, can also cause your premiums to go up.

Return-to-work programs

A smart return-to-work program could be the answer. The idea is that by bringing injured workers back to the workforce, with whatever modifications they need, the employer can realize at least some value. In the long run, your company pays either way – either in wages and benefits to an employee working at a reduced productivity level, or in future workers' comp lost-wages claims.

Before you do so, though, count the costs.

You not only have wages to pay ... you are also paying benefits and taxes on a less productive employee.

But what about the intangible effects of bringing the employee back? Is the worker disgruntled? Is he blaming management? Will he cause morale issues by complaining to fellow workers about incompetent or uncaring management when that's simply not the case?

And how will workers perceive him? Will a worker placed on light duty in an air-conditioned office cause employees to think he's "getting one over?" Could it inspire copycat claims from others hoping for the same cushy deal?

And, once you bring a worker back on light duty at full pay, what is the incentive to increase productivity? Have you removed the incentive to perform?

In this case, you have substantially reduced the risk to the insurance company of course – but only by taking more and more of the cost on yourself directly, which defeats the purpose of having insurance in the first place.

Aggravated injuries

If a worker has one injury, they are at an elevated risk of a repeat injury or an aggravation of the pre-existing injury.

If you have a worker with, say, a moderate back injury, and you put her back to work, you run a real risk that she will re-injure herself – possibly causing an even more expensive claim.

Savings

The savings from a well-constructed return-to-work program are well documented. Most workers want to be productive, and employers are frequently resourceful in finding injured workers something of value they can do while they recover.

Furthermore, simply having a program in place – and a record of having made a reasonable offer of employment to an injured worker – can significantly strengthen the hand of the employer if the worker should take legal action.

Judges will frequently disallow workers' comp claims if the employee is on record as declining a reasonable work offer, taking their physical capabilities into account.

The takeaway

Return-to-work programs are valuable, but they're not the best solution in every single case.

They work best where the employer/employee relationship is strong, where you have generally well-motivated and honest employees who take pride in their work, and where you have adequate controls in place for reporting and documenting injuries right from the beginning.

It's important to have a good return-to-work program on the books, documented in your employee manuals. But always treat each case on its own merits, taking into account the individual circumstances involved. ❖